aws

User Guide

Amazon Q Business

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Q Business: User Guide

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

..... xiv

What is Amazon Q Business? 1

Benefits of Amazon Q Business 1

Pricing and availability 3

Accessing Amazon Q Business 3

Related services 4

Are you a first-time Amazon Q Business user? 4

Getting started 6

How Amazon Q Business works 6

Admin workflow 7

User workflow 10

Amazon Q Business workflow 11

Key concepts 12

Agentic RAG 13

Application environment 14

ACLs (Access Control Lists) 14

Amazon Q Apps 14

Analytics dashboard 14

Audio and video extraction 15

Browser extensions 15

Chat orchestration 15

Custom document enrichment 15

Data accessors 15

Data source 16

Data source connector 16

Document 16

Document attributes 16

Field mappings 16

Filtering using document attributes 17

Foundation model 17

Guardrails 17

Hallucination 17

Hallucination mitigation 17

IAM Identity Center 18

Identity Federation through IAM ... 18
Identity provider ... 18
Index ... 18
Index capacity ... 18
Integrations ... 19
ISV integration ... 19
Large language model ... 19
Principal Mapping ... 19
Plugins ... 20
Quick prompts ... 20
Response personalization ... 20
Retriever ... 20
Retrieval Augmented Generation ... 20
Relevance tuning ... 21
Subscription tiers ... 21
Tags ... 21
Visual content extraction ... 21
User store ... 22
Web experience ... 22
Subscription tiers and index types ... 22
Index types ... 22
User subscription tiers ... 23
Understanding user subscriptions ... 27
Pricing ... 27
Supported document formats ... 28
Supported document types ... 29
Document attributes and types ... 32
Types of document attributes ... 32
Mapped document attributes ... 34
Document attribute data types ... 35
Supported languages ... 35
Setting up ... 35
Initial AWS account setup ... 36
(Optional) Install the AWS CLI ... 38
(Optional) Set up the AWS SDKs ... 38
Consider AWS Regions and endpoints ... 39

Set up required permissions ... 40
IAM roles ... 43
Amazon Q Business application ... 44
Amazon Q Business web experience ... 48
Data source connectors ... 72
Plugins ... 85
Custom document enrichment ... 87
Amazon Kendra retriever ... 93
Creating an IAM Identity Center-integrated application ... 95
Configuring an IAM Identity Center instance ... 96
Prerequisites ... 96
Understanding IAM Identity Center instances ... 97
Creating a same-region integration ... 99
Creating a cross-region integration ... 99
Creating an application environment ... 101
Migrating an application to IAM Identity Center ... 108
Migrating an application ... 109
Using APIs to create an application ... 114
Using APIs to create an application ... 114
Prerequisites ... 116
One-time setup ... 116
Workflow for custom application backend API calls for an authenticated user ... 121
Managing resources ... 125
Managing applications ... 125
Managing web experiences ... 129
Managing subscriptions ... 133
Tagging resources ... 137
Creating an IAM federated application ... 140
Using Okta for IAM federation ... 141
Prerequisites ... 142
Step 1: Create and configure an Okta application ... 143
Step 2: Add an identity provider in IAM ... 148
Step 3: Connect IAM to Okta ... 152
Step 4: Create Amazon Q Business application ... 154
Using Microsoft Entra ID for IAM federation ... 158
Prerequisites ... 159

Step 1: Create and configure a Microsoft Entra ID application 160
Step 2: Create an IAM identity provider 162
Step 3: Update your Microsoft Entra ID application with the IAM role ARN 164
Step 4: Create an Amazon Q Business application 166
Step 5: Update your Microsoft Entra ID application with the web experience URL 169
Troubleshooting Microsoft Entra ID integration 169
Connecting multiple Amazon Q Business applications to a single IdP 171
Using SAML 171
Using OIDC 173
Using APIs to create an IAM federated application 173
Prerequisites 174
One-time setup 174
Workflow for each API call session for authenticated user 175
Managing resources 176
Managing applications 176
Managing web experiences 180
Managing subscriptions 184
Tagging resources 188
Creating anonymous access application 191
Creating an anonymous access application environment 192
Using APIs to create an application environment 195
Prerequisites 196
One-time setup 196
Workflow for each API call session 121
Managing resources 197
IAM policies 198
Managing anonymous application environments 202
Managing web experiences 206
Creating an Amazon Quick-integrated application 211
Considerations 211
Creating a Quick-integrated application from Amazon Quick 212
Creating a Quick-integrated application with Amazon Q Business API operations 212
Enhancing an application 214
Data sources 215
Creating an index 216
Uploading files 221

Adding data connectors ... 223
Troubleshooting data source connectors ... 2709
Managing resources ... 2714
Admin controls and guardrails ... 17
Key terms ... 2737
Using global controls ... 2738
Using topic-level controls ... 2745
Managing admin controls and guardrails ... 2749
Response customization ... 2751
Response customization settings ... 2751
Managing response configurations ... 2755
Data accessors ... 15
Verified data accessors ... 2761
Prerequisites ... 2762
Add data accessor ... 2763
Completing the process ... 2771
Removing access ... 2773
Amazon Q embedded ... 2774
Prerequisites ... 2775
Add your website as an allowed URL ... 2775
Add Amazon Q embedded to your website ... 2776
Remove your website as an allowed URL ... 2777
Integrations ... 19
Browser extensions ... 15
Slack ... 2787
Microsoft Teams ... 2795
Microsoft Outlook ... 2802
Microsoft Word ... 2809
IAM Roles and Trust Policy ... 2816
Amazon Q Apps ... 2820
Prerequisites for Amazon Q Apps ... 2821
Managing Amazon Q Apps ... 2823
Creating Amazon Q Apps ... 2823
Sharing Amazon Q Apps ... 2825
Custom labels for Amazon Q Apps ... 2829
Verified Amazon Q Apps ... 2832

Amazon Q Apps data collection ... 2834
Using plugins in Amazon Q Apps ... 2842
Document enrichments ... 2846
Document enrichment limitations ... 2847
How document enrichment works ... 2848
Using basic operations ... 2850
Using Lambda functions ... 2859
Extracting semantic meaning from visuals ... 2883
End user experience ... 2884
Guidelines and requirements ... 2884
Extracting content from visuals with data connectors ... 2885
Extracting semantic meaning from audio and video content ... 2886
Extracting content from visuals in a file ... 2889
Downloading images to add to responses (API operations) ... 2890
Relevancy tuning ... 2891
Recency ... 2892
Sources ... 2892
Rank order ... 2892
Setting relevancy preferences ... 2893
Metadata boosting (Legacy) ... 2895
Understanding boosting (Legacy) ... 2897
Boosting types (Legacy) ... 2898
Configuring document attributes for boosting (Legacy) ... 2901
Enabling document attributes for search (Legacy) ... 2905
Metadata controls ... 2909
Mapping document attributes directly to index fields ... 2910
Mapping data source document attributes to index fields ... 2912
Ingesting attributes using the BatchPutDocument API operation ... 2914
Using aggregations and dynamic filtering in chat ... 2915
Customizing a web experience ... 2916
Overview ... 2917
Text Elements ... 2917
Console ... 2917
CLI ... 2918
Visual Themes ... 2918
Prerequisites ... 2919

Console ... 2921
CLI ... 2922
Reference Materials ... 2922
Accessibility ... 2922
Color Values ... 2922
CSS Variables ... 2923
Example ... 2924
Configuring actions ... 2925
Quick plugin ... 2926
Pricing ... 2927
Guidelines and requirements ... 2928
Service access role ... 2928
Configuring the plugin ... 2929
Getting data insights from Amazon Quick answers ... 2932
Pausing integration with Quick ... 2933
Built-in plugins ... 2934
Prerequisites ... 2935
Asana ... 2938
Atlassian Confluence ... 2942
Google Calendar ... 2946
Jira Cloud ... 2950
Microsoft Exchange ... 2955
Microsoft Teams ... 2959
PagerDuty Advance ... 2963
Salesforce ... 2968
ServiceNow ... 2973
Smartsheet ... 2978
Zendesk Suite ... 2982
Jira (Legacy) ... 2986
Salesforce (Legacy) ... 2990
ServiceNow (Legacy) ... 2993
Zendesk (Legacy) ... 2997
Using built-in plugins ... 3000
Custom plugins ... 3004
Prerequisites ... 3005
Service access roles ... 3005

Defining OpenAPI schemas ... 3007
Best practices for OpenAPI schema definition ... 3013
Creating a custom plugin ... 3026
Using a custom plugin ... 3029
Managing plugins ... 3032
Updating a plugin ... 3032
Deleting a plugin ... 3034
Getting plugin properties ... 3035
Listing plugins ... 3035
Listing configured plugin actions ... 3036
Listing available plugin actions ... 3037
Listing plugin metadata ... 3038
Amazon Q Business features ... 3039
Filtering using document attributes and metadata ... 3040
Source attribution with citations ... 3041
Upload files and chat ... 3042
Personalizing chat responses ... 3043
Quick prompts ... 3043
Hallucination mitigation ... 3043
Agentic RAG ... 3044
Using a web experience ... 3046
Example prompts ... 3047
Engage with contextual responses ... 3047
Analysis and reasoning ... 3047
Perform actions using plugins ... 2925
Review source citations ... 3048
Upload files and chat ... 3048
Advanced search ... 3049
Copy responses ... 3049
Provide feedback ... 3049
Conversation management ... 3050
Response sources ... 3050
Login, Logout and session duration for Web Experience ... 3050
Amazon Q index for ISVs ... 3052
Key concepts ... 3052
Prerequisites ... 3053

ISV information ... 3056
Getting access ... 3060
Customer grants access ... 3060
ISV setup ... 3061
Access as a dataaccessor ... 3062
Data retrieval ... 3062
Creating an Amazon Q index ... 3067
Identity management ... 3067
SearchRelevantContent - IDC ... 3068
SearchRelevantContent - IAM Federation ... 3069
Troubleshooting ... 3071
Security ... 3072
Data protection ... 3073
Data encryption for Amazon Q Business ... 3074
Data encryption for Q Apps ... 3085
Key management ... 3087
Cross-region inference ... 3087
Service improvement ... 3089
Amazon VPC endpoints (AWS PrivateLink) ... 3089
Creating an interface VPC endpoint for Amazon Q Business ... 3089
Creating a VPC endpoint policy for Amazon Q Business ... 3090
Identity and access management ... 3091
Audience ... 3091
Authenticating with identities ... 3092
Managing access using policies ... 3093
How Amazon Q Business works with IAM ... 3094
Identity-based policy examples ... 3101
AWS managed policies ... 3109
AWS managed policies for Q App ... 3113
Using service-linked roles ... 3115
Using service-linked roles for Q Apps ... 3120
Troubleshooting ... 3122
Compliance validation ... 3124
Using ACL Analyzer ... 3124
Prerequisites ... 3124
Getting Started with ACL Analyzer ... 3125

Configuring Data Sources ... 3126
Using the ACL Analyzer Tool ... 3126
Resilience ... 3127
Infrastructure security ... 3128
Cross-service confused deputy prevention ... 3128
Configuration and vulnerability analysis ... 3129
Security best practices ... 3130
Apply principle of least privilege ... 3130
Role-based access control (RBAC) permissions ... 3130
Monitoring ... 3131
Amazon Q Business CloudTrail logs ... 3132
Amazon Q Business information in CloudTrail ... 3132
Control plane events in CloudTrail ... 3133
Data plane events in CloudTrail ... 3134
Amazon Q Business management events in CloudTrail ... 3137
Understanding Amazon Q Business log file entries ... 3137
Amazon Q Apps CloudTrail logs ... 3139
Amazon Q Apps information in CloudTrail ... 3139
Management events ... 3140
Data events ... 3141
UnderstandingAmazon Q Apps log file entries ... 3143
CloudWatch metrics ... 3144
Using CloudWatch Metrics ... 3145
Viewing metrics ... 3146
Creating a CloudWatch alarm ... 3147
Amazon Q Business chat metrics ... 3148
Amazon Q Business API operation metrics ... 3151
Amazon Q Business index metrics ... 3152
Amazon Q Apps metrics ... 3153
Amazon Q Business CloudWatch Logs ... 3155
Log examples ... 3156
Permissions ... 3158
Enabling logging ... 3159
Log query examples ... 3162
Analytics dashboards ... 14
Viewing the analytics dashboards ... 3164

Amazon Q Business Analytics dashboard metrics 3165
Amazon Q Apps Analytics dashboard metrics 3169
Maintenance updates 3171
Amazon Q Business index updates 3171
Service quotas 3173
Supported Regions 3173
Quotas 3175
API reference 3180
Creating an application 3181
Creating an index 3182
Creating a retriever 3182
Connecting a data source 3183
Upload documents directly 3184
GetDocumentContent Output Schema 3185
Example Output 3187
Creating a web experience 3187
Chat and conversation management 3188
Setting up a streaming chat 3189
User and group management 3201
Subscription management 3202
Plugins 3203
Admin controls and guardrails 3205
User feedback 3205
Document history 3206

What is Amazon Q Business?

Powered by Amazon Bedrock: AWS implements automated abuse detection. Because Amazon Q Business is built on Amazon Bedrock, users can take full advantage of the controls implemented in Amazon Bedrock to enforce safety, security, and the responsible use of artificial intelligence (AI).

Amazon Q Business is a fully managed, generative-AI powered assistant that you can configure to answer questions, provide summaries, generate content, and complete tasks based on your enterprise data. It allows end users to receive immediate, permissions-aware responses from enterprise data sources with citations, for use cases such as IT, HR, and benefits help desks.

Amazon Q Business also helps streamline tasks and accelerate problem solving. You can use Amazon Q Business to create and share task automation applications, or perform routine actions like submitting time-off requests and sending meeting invites.

Amazon Q Business integrates with services like Amazon Kendra and other supported data sources such as Amazon S3, Microsoft SharePoint, and Salesforce.

To get started with Amazon Q Business, visit Amazon Q Business.

What is Amazon Q Business?

Topics

- Benefits of Amazon Q Business
- Pricing and availability
- Accessing Amazon Q Business
- Related services
- Are you a first-time Amazon Q Business user?

Benefits of Amazon Q Business

Some of the benefits of Amazon Q Business include:

Accurate and comprehensive answers

Amazon Q Business generates comprehensive responses to natural language queries from users by analyzing information across all enterprise content that it has access to. It can avoid incorrect statements by confining its generated responses to existing enterprise data, and provides citations to the sources that it used to generate its response. When a query results in conflicting or inconsistent answers, Amazon Q Business lists the details for each answer. With hallucination mitigation, Amazon Q Business checks supported chat responses for inconsistencies and automatically corrects them in real-time during conversations.

Simple to deploy and manage

Amazon Q Business takes care of the complex task of developing and managing machine learning infrastructure and models so that you can build your chat solution quickly. Amazon Q Business connects to your data and ingests it for processing using its pre-built connectors, document retrievers, document upload capabilities.

Configurable and customizable

Amazon Q Business provides you with the flexibility of choosing what sources should be used to respond to user queries. You can control whether the responses should only use your enterprise data, or use both enterprise data and model knowledge. For public-facing scenarios, you can create anonymous applications that don't require user authentication, allowing you to serve a broader audience. You can customize your chat interface with your organization's branding, visual themes, and conversation starters to create a tailored user interface.

Data and application security

Amazon Q Business supports access control for your data so that the right users can access the right content. Its responses to questions are based on the content that your end user has permissions to access. You can use AWS IAM Identity Center or AWS Identity and Access Management to manage end user access for Amazon Q Business.

Broad connectivity

Amazon Q Business offers out-of-the-box connections to multiple supported data sources. You can also connect Amazon Q to any third-party application using plugins to perform actions and query application data. With data accessors, you can securely share your enterprise data with verified ISVs, allowing them to retrieve relevant content from your Amazon Q index. Amazon Q Business integrations bring AI-powered assistance directly into daily workflows through browser extensions and applications for Slack, Microsoft Teams, and Microsoft Office. You can

also embed Amazon Q Business directly into your applications and websites to enhance user productivity.

Pricing and availability

Amazon Q Business charges you both for user subscriptions to applications, and for index capacity. For information about what's included in the tiers of user subscriptions and index capacity, see Subscription and index pricing.

For pricing information, including examples of charges for index capacity, subscribing and unsubscribing users to Amazon Q Business tiers, upgrading and downgrading Amazon Q Business tiers, and more, see Amazon Q Business Pricing.

For a list of regions where Amazon Q Business is currently available, see Supported regions.

Accessing Amazon Q Business

You can access Amazon Q Business in the following ways in the AWS Regions that it's available in:

AWS Management Console

You can use the AWS Management Console—a browser-based interface to interact with AWS services—to access the Amazon Q Business console and resources. You can perform most Amazon Q Business tasks using the Amazon Q Business console.

Amazon Q Business API

To access Amazon Q Business programmatically, you can use the Amazon Q API. For more information, see the Amazon Q Business API Reference.

AWS Command Line Interface

The AWS Command Line Interface (AWS CLI) is an open source tool. You can use the AWS CLI to interact with AWS services using commands in your command line shell. If you want to build task-based scripts, using the command line can be faster and more convenient than using the console.

SDKs

AWS SDKs provide language APIs for AWS services to use programmatically.

Related services

The following are some of the other AWS services that Amazon Q Business integrates with:

Amazon Kendra

Amazon Kendra is an intelligent search service that uses natural language processing and machine learning algorithms to return specific answers from your data for end user queries. If you're already an Amazon Kendra user, you can use Amazon Kendra as a data retriever for your Amazon Q Business web application.

Amazon S3

Amazon S3 is an object storage service. If you're an Amazon S3 user, you can use Amazon S3 as a data source for your Amazon Q Business application.

Quick

Quick is a business intelligence service that helps you create and share interactive dashboards and reports. You can integrate Amazon Q Business with Quick to enable users to ask natural language questions about their data and receive AI-generated insights directly within their dashboards.

Are you a first-time Amazon Q Business user?

If you're a first-time user of Amazon Q Business, we recommend that you read the following sections in order:

How it works

Introduces Amazon Q Business components and describes how they work to create your Retrieval Augmented Generation (RAG) solution.

Key concepts

Explains key concepts and important Amazon Q Business terminology.

Setting up

Outlines how to set up Amazon Q Business so that you can begin creating your Amazon Q Business application and web experience.

Creating an application

Explains how to create the Amazon Q Business application integrated with IAM Identity Center.

Connecting Amazon Q Business data source connectors

Configuration information for specific connectors to use with your Amazon Q Business web experience.

Getting started with Amazon Q Business

To start using Amazon Q Business, set up an AWS account and create the necessary AWS Identity and Access Management (IAM) users and roles. To use the AWS Command Line Interface (AWS CLI) or the AWS SDKs, you must install and configure them. After learning about Amazon Q concepts and setting up, you are ready to begin creating your application.

> **Note**
>
> Amazon Q Business does not use customer data for service improvement or for improving underlying LLMs.

Topics

- How Amazon Q Business works
- Key concepts of Amazon Q Business
- Amazon Q Business subscription tiers and index types
- Supported document formats in Amazon Q Business
- Document attributes in Amazon Q Business
- Supported languages for Amazon Q Business
- Setting up for Amazon Q Business
- IAM roles for Amazon Q Business

How Amazon Q Business works

With Amazon Q Business, you can build an interactive chat application environment for your organization's end users, using a combination of your enterprise data and large language model knowledge, or enterprise data only. The following sections outline how Amazon Q works.

Topics

- Admin workflow
- User workflow
- Amazon Q Business workflow

Admin workflow

Amazon Q Business uses AWS IAM Identity Center to connect to your workforce users. Identity Federation through IAM is also supported, with the limitations described below. If you're an admin user configuring an Amazon Q Business application, your application creation process depends on whether you're using IAM Identity Center or AWS Identity and Access Management for end user access management.

If IAM Identity Center is already enabled in your organization, Amazon Q Business will automatically identify it and allow you to connect to it. IAM Identity Center will enable you to manage access based on the users and groups in your corporate directory. It will provide you with accurate billing for the subscriptions of your users and will ensure that your configuration can support the future growth of your Amazon Q Business use cases.

If IAM Identity Center is not yet enabled, we strongly recommend that you work with your AWS Administrator to enable an organization instance of IAM Identity Center. This will give your AWS Administrator the most control over the configuration. It will ensure accurate billing for the subscriptions of your users. It will also give you the most flexibility to grow Amazon Q Business use cases, spanning multiple AWS accounts, users, and integrations with other AWS applications. If your AWS Administrator cannot enable an organization instance of IAM Identity Center, you can enable an account instance of IAM Identity Center by yourself through the Amazon Q Business console. Your deployment of Amazon Q Business, and its integration with other AWS applications, will be limited to the AWS Region and AWS account where the IAM Identity Center account instance is enabled.

> **Note**
>
> If you have Amazon Q Business deployments with account instances of IAM Identity Center in multiple AWS accounts, you will be billed separately for user subscriptions per AWS account. For more information, see Understanding user subscriptions.

If you cannot use any IAM Identity Center option, you can still set up Amazon Q Business using IAM Federation through OIDC (preferred) or SAML. This approach will give your users access to Amazon Q Business capabilities, but will limit your ability to scale Amazon Q Business use cases via integration with other AWS applications.

> **Note**
>
> If you have Amazon Q Business deployments with IAM federation to multiple AWS accounts, you will be billed separately for user subscriptions per AWS account. For more information, see Understanding user subscriptions.

The following section outlines the admin workflow for creating applications with IAM Identity Center and Identity Federation through IAM.

Topics

- Admin workflow for apps using AWS IAM Identity Center
- Admin workflow for apps using Identity Federation through IAM

Admin workflow for apps using AWS IAM Identity Center

Amazon Q Business supports managing end user access to applications using AWS IAM Identity Center. When you use AWS IAM Identity Center to manage users, you sync user identities into IAM Identity Center and connect your Amazon Q Business to IAM Identity Center to manage user access.

As an admin user using IAM Identity Center for user management—including integrating an external identity provider to manage user access through IAM Identity Center—you create and configure an Amazon Q Business application environment by completing the following steps:

1. Enabling an IAM Identity Center instance and connecting the identity source for your Amazon Q Business application environment in IAM Identity Center. Amazon Q Business supports both organization and account level IAM Identity Center instances.
2. Connecting an IAM Identity Center instance for your Amazon Q Business application environment with users and groups added.
3. Creating a fully-configured Amazon Q Business application that powers your web experience, connected to IAM Identity Center.

   If you use the console to create an application environment, Amazon Q Business automatically creates a web experience for you, unless you choose not to. If you use the API, you have to create a web experience for your application environment.

> **Note**
>
> When you create an application, you can optionally add groups and users who will be able to access the Amazon Q Business web experience, and then provision the user subscriptions. Or, you can add groups and users when you update your application. An Amazon Q application environment will be created even if you don't add users to it, but an application environment needs to have a subscribed user to work.

> **Important**
>
> Only an admin can create and upgrade user subscriptions.

4. (Optional) Enhancing the web experience by adding data sources to it, configuring admin-level controls, tuning chat relevance, plugins, and chat features (including Amazon Q Apps) for end users. For more information, see Enhancing an Amazon Q Business application environment and Amazon Q Business features.
5. (Optional) Customizing your web experience to test how it looks for your end users. In this step, you add a title and subtitle for your web experience, a welcome message, and quick prompts for your end users. You can't chat with—or test—the application environment in customize mode.
6. Then, share the web experience URL generated by Amazon Q Business with the end users you've subscribed so that they can log in and begin chatting.

> **Note**
>
> When you create an application, response generation from large language model (LLM) knowledge is enabled by default.

Admin workflow for apps using Identity Federation through IAM

Amazon Q Business supports managing end user access to applications using Identity Federation through IAM. When you use IAM Identity Federation to manage users, your application derives user identities directly from your identity provider. As an admin, you create and configure a Amazon Q Business application environment using IAM Identity Federation by completing the following steps:

1. Configuring your external identity provider and connecting it to an AWS Identity and Access Management identity provider instance.
2. Creating a fully-configured Amazon Q Business application that powers your web experience, connected to your identity provider through IAM. You also add subscriptions for end users by adding subscriptions when you create an application.
3. (Optional) Enhancing the web experience by adding a data source, configuring admin-level controls, tuning chat relevance, plugins, and chat features (including Amazon Q Apps) for end users. For more information, see Enhancing an Amazon Q Business application environment and Amazon Q Business features.
4. Optionally, customizing your web experience to test how it looks for your end users. In this step, you add a title and subtitle for your web experience, a welcome message, and quick prompts for your end users. You can't chat with—or test—the application environment in customize mode.
5. Then, sharing either your own custom web application URL or the web experience URL generated by Amazon Q Business with the end users you've subscribed so that they can log in and begin chatting.

> **Note**
>
> When you create an application, response generation from large language model (LLM) knowledge is enabled by default.

User workflow

If you're an end user using your organization's Amazon Q Business web experience, you perform the following steps:

1. Navigate to your organization's Amazon Q Business web experience URL, and sign in with your credentials.
2. Start chatting and ask questions of your organization's Amazon Q Business web experience. You can, for example choose from the following options:
   - **Ask questions** – Ask a question. Amazon Q Business generates and returns answers based on the enterprise data that the end user has access to. Continue the conversation by asking follow-up questions.
   - **Verify response sources** – Each Amazon Q Business answer cites the source documents used to generate it.

- **See conversation history** – Amazon Q Business retains conversation history for 30 days so that they can search through questions and answers. You can view conversation history from the left navigation pane.
- **Summarize content** – Amazon Q Business can summarize email message threads.
- **Create outlines and drafts** – Use Amazon Q Business to create outlines and templates for documents.
- **Perform plugin actions** – If you've configured Plugins, ask Amazon Q Business to perform actions on your behalf, like creating a ticket in a supported third party app.
- **Test guardrails and chat controls** – If you've configured Guardrails and chat controls, check how Amazon Q Business responds to queries and special topics.
- Additionally, you can ask Amazon Q Business to complete any supported follow-up tasks—like creating task-focused Amazon Q Apps—that your admin has enabled for your application environment.

For a list of web experience capabilities, see Using an Amazon Q web experience.

3. Sometimes your question requires information that's beyond the scope of your enterprise data. Then, Amazon Q Business responds that it couldn't find an answer in your documents, unless your admin has allowed Amazon Q Business to generate responses using model knowledge.

Amazon Q Business stores conversation history for 30 days and maintains conversation context after a conversation ends. Conversations can be resumed from where you left off within this 30-day period.

Amazon Q Business workflow

In response to an end user query during a web experience chat, Amazon Q Business does the following:

1. Uses the retriever chosen by the admin to select and retrieve documents that are relevant to the query, following authorization and access control.
2. Generates a response to the user query using either a combination of retrieved enterprise data and model knowledge, or only enterprise data, depending on admin configuration.
3. Returns the generated response to the end user. Amazon Q Business assigns a unique message ID to each answer for tracking purposes.

Key concepts of Amazon Q Business

This section describes the key concepts and terms related to Amazon Q Business.

Topics

- Agentic RAG
- Application environment
- ACLs (Access Control Lists)
- Amazon Q Apps
- Analytics dashboard
- Audio and video extraction
- Browser extensions
- Chat orchestration
- Custom document enrichment
- Data accessors
- Data source
- Data source connector
- Document
- Document attributes
- Field mappings
- Filtering using document attributes
- Foundation model
- Guardrails
- Hallucination
- Hallucination mitigation
- IAM Identity Center
- Identity Federation through IAM
- Identity provider
- Index
- Index capacity

- Integrations
- ISV integration
- Large language model
- Principal Mapping
- Plugins
- Quick prompts
- Response personalization
- Retriever
- Retrieval Augmented Generation
- Relevance tuning
- Subscription tiers
- Tags
- Visual content extraction
- User store
- Web experience

Agentic RAG

Agentic RAG (Retrieval Augmented Generation) is an advanced natural language processing technique that enhances Amazon Q Business's standard RAG capabilities. Using Agentic RAG, Amazon Q Business employs multiple intelligent agents and specialized tools to process queries and retrieve and generate responses from your enterprise data using its underlying large language model, while continuously monitoring quality.

With Agentic RAG system processes queries through a combination of the following coordinated steps:

- Analyzes both the user's question and conversation history and determines which retrieval tools to use
- Intelligently triggers multiple retrieval operations as needed
- Synthesizes information from various sources, and generate responses using its underlying large language model

For more information, see Agentic Retrieval Augmented Generation (RAG).

Application environment

An Amazon Q Business application environment is the primary resource that you use to create a chat solution. To create the application environment, you can use either the Amazon Q Business console or Amazon Q Business API actions. Amazon Q Business offers four distinct methods for creating applications: the standard approach with IAM Identity Center integration, an IAM federation option for AWS-centric environments, an anonymous application method for public-facing scenarios, and a specialized Quick integration for analytics-focused implementations. Each creation pathway provides different authentication mechanisms and integration capabilities, allowing organizations to select the most appropriate solution based on their security requirements and existing infrastructure.

ACLs (Access Control Lists)

ACLs control user and system actions for resources. Users can read, write, execute, or modify data based on ACL permissions.

Amazon Q Apps

Amazon Q Business allows web experience users to create lightweight, purpose-built Q Apps to fulfill specific tasks from within their web experience. For example, you can use Amazon Q Business to create an app with a web experience that exclusively generates marketing-related content to improve your marketing team's productivity. Your marketing team members can, in turn, also create their own Amazon Q Apps with its own marketing content-generation capabilities—like writing customer emails and creating promotional content using a certain style of voice, tone, and branding. For more information, see Amazon Q Apps.

Analytics dashboard

The Amazon Q Business analytics dashboard provides comprehensive insights into how users interact with your application. It offers metrics and visualizations on conversation volumes, popular topics, user engagement patterns, and system performance. Administrators can use these analytics to identify trends, understand user needs, measure adoption rates, and make data-driven decisions to improve the application. The dashboard helps track the effectiveness of your Amazon Q Business implementation, identify areas for enhancement, and demonstrate the value it brings to your organization. For more information, see Using the analytics dashboard.

Audio and video extraction

Amazon Q Business extracts semantic information from audio and video files, making multimedia content queryable. This allows users to query audio and video content using natural language and explore deeper with follow-up questions, enhancing information retrieval from multimedia sources. For more information, see Extracting semantic meaning from audio and video content.

Browser extensions

The Amazon Q Business browser extension enhances users' web browsing experience by bringing AI-powered assistance directly into their daily workflows. Available for Google Chrome, Microsoft Edge, and Mozilla Firefox browsers, the extension allows users to summarize web pages, ask questions about content, access company knowledge, and use other features available in the Amazon Q Business web experience. This integration requires installation and authentication. For more information, see Enhancing web browsing with Amazon Q Business.

Chat orchestration

Chat orchestration is a Amazon Q Business feature that automatically manages chat requests across configured plugins and data sources. When enabled, Amazon Q Business automatically routes chat requests to plugins, integrating enterprise data and relevant actions within a single chat response. This feature provides unified response integration combining RAG workflow with plugin actions, intelligent action detection for read-only vs. write actions, and smart plugin management with user-driven experience through clarification requests when needed. For more information, see Chat orchestration settings.

Custom document enrichment

Document enrichment is an Amazon Q Business feature that you can use to manipulate your document content and document attributes. You can use document enrichment to perform optical character recognition (OCR) or translation. Document enrichment uses basic and Lambda operations. For more information see, Document attributes and types and Document enrichment.

Data accessors

The Amazon Q Business data accessors feature allows you to securely share your enterprise data with verified independent software vendors (ISVs) using Amazon Q. This feature enables ISVs to retrieve relevant content from your Amazon Q index, enhancing their applications with your

organization's knowledge. By granting controlled access to your data, you can leverage third-party tools while maintaining security and data access compliance. Data accessors include verified software providers such as Asana, Miro, Zoom, PagerDuty, and Planview. For more information, see Share your enterprise data with data accessors.

Data source

A data source is a document repository.

Data source connector

A data source connector can crawl and synchronize a data source with an Amazon Q Business index at customizable intervals. Amazon Q Business supports multiple connectors so that you can build your generative AI solution with minimal configuring. For a list of Amazon Q Business supported connectors, see Supported connectors. For an overview of Amazon Q Business connector features, see Amazon Q Business data source connector features.

Document

In Amazon Q Business, a document is a unit of data. Specific document formats supported include .csv, .docx, HTML, JSON, .pdf, plaintext, .ppt, .pptx, .rtf, and .xslx. For more information, see Supported document types.

Document attributes

Document attributes are structural metadata associated with documents, such as document title, document type, and date and time created. Amazon Q Business extracts document attributes during the document ingestion process to provide customizable chat and data manipulation capabilities for your application environment. Amazon Q Business offers reserved document attributes that you can use. Or, you can create custom attributes. For more information, see Document attributes, Filtering using document attributes, Boosting using document attributes, and Custom document enrichment.

Field mappings

An Amazon Q Business index has fields that help you structure data to aid the retrieval process. You can map index fields to your document attributes when you add documents directly to an index, or use a data source connector.

Filtering using document attributes

Filtering using document attributes is an Amazon Q Business feature that you can use to filter your Amazon Q Business chat responses for your end user. For example, if you have a document attribute associated with a data source type, you can use the attribute to mandate that chat responses only be generated from a specific data source. For more information, see Filtering using document attributes.

Foundation model

A foundation model (FM) is a broad, function-based machine learning model (not specific to language systems). An FM is tuned to a large number (billions) of parameters and is trained on a large corpus of documents.

Guardrails

An Amazon Q Business feature that lets you define global controls and topic-level controls for your application environment. Using this feature, you can control what sources your application environment will use to generate responses from, and also control what topics it will respond to and how. For more information, see Guardrails.

Hallucination

A hallucination, in the machine learning context, is a confident response by an AI application environment that isn't justified by its training data. Think of a hallucination as instances where the response doesn't make sense in the context of the prompt, or when the responses are out of scope with the documents provided. Amazon Q Business offers you the ability to minimize hallucinations by allowing your retrieval system to generate responses only from your existing enterprise data.

Hallucination mitigation

Hallucination mitigation is a Amazon Q Business feature that checks chat responses for hallucinations and corrects inconsistencies in real-time during chat. If a hallucination is detected with high confidence, Amazon Q Business corrects the inconsistencies in its response and generates a new, edited message. This feature is only available for retrieval augmented generation (RAG) responses from data connected to the application and is not supported for chat orchestration, plugin workflows, or responses generated from tabular data or multimedia transcripts. For more information, see Response settings.

IAM Identity Center

You can manage user access to your Amazon Q Business application environment using IAM Identity Center as your AWS gateway to the identity provider of your choice. For more information on creating an Amazon Q Business application environment integrated with IAM Identity Center see Configuring an IAM Identity Center instance and Configuring an Amazon Q Business application. For more information about using IAM Identity Center to manage access to applications, see Manage access to applications in the IAM Identity Center User Guide.

Identity Federation through IAM

Amazon Q Business supports identity federation through AWS Identity and Access Management. When you use identity federation, you can manage users with your enterprise identity provider (IdP) and use AWS Identity and Access Management to authenticate users when they sign in to AWS Identity and Access Management. For more information on creating an Amazon Q Business application environment integrated with AWS Identity and Access Management see Configuring an Amazon Q Business application.

Identity provider

An identity provider (IdP) is a service that stores, manages, maintains, and verifies user identities for your application environment (in this case, Amazon Q Business). Some examples of IdPs are IAM Identity Center, Okta, and Microsoft EntraID (formerly Azure Active Directory).

Index

An index is a corpus of documents. Amazon Q Business supports its own index where you can add and sync documents. An index has fields that you can map your document attributes to, to enhance your end user's chat experience. Amazon Q Business creates retriever for you when it creates your Amazon Q Business index. Amazon Q Business provides two types of index: Enterprise and Starter.

You can also use an Amazon Kendra index as a retriever for your generative AI application environment.

Index capacity

When you use an Amazon Q Business native index for your application environment, you must provision data storage capacity for it. Amazon Q Business provides two types of index: Enterprise

and Starter. Both index types include 20,000 documents or 200 MB of total extracted text (whichever is reached first) and 100 hours of data connector usage (time that it takes to scan and index new, updated, or deleted documents) by default. For more information, see Amazon Q Business Index types and Pricing for subscriptions and indices.

Integrations

Amazon Q Business integrations enhance user productivity by bringing AI-powered assistance directly into daily workflows through third-party enterprise tools. These integrations include browser extensions for Google Chrome, Microsoft Edge, and Mozilla Firefox browsers, as well as applications for Slack, Microsoft Teams, Microsoft Outlook, and Microsoft Word. Each integration must be configured and deployed to bring Amazon Q Business capabilities directly within those enterprise tools, allowing users to access Amazon Q's knowledge without context switching during their work. For more information, see Integrations.

ISV integration

Amazon Q Business enables independent software vendors (ISVs) to leverage customer enterprise data through the Amazon Q index to enhance their applications with generative AI capabilities. ISVs can access this data through two methods: either by being added as a data accessor to an existing customer's Amazon Q index, or by creating a Amazon Q application on behalf of the customer. The `SearchRelevantContent` API operation allows ISVs to retrieve relevant content from the customer's data sources while maintaining security and access controls, ensuring users only see content they have permission to access. This integration enables software providers to build enhanced application experiences without having to directly connect to or index individual data sources. For more information, see Amazon Q index for independent software vendors (ISVs).

Large language model

A large language model (LLM) is a language-based, machine learning model that's tuned to a large number (billions) of parameters and trained on a large corpus of documents.

Principal Mapping

Principal mapping is used to connect users and groups with their user ids and group membership information in data sources connected to the application.

Plugins

Amazon Q Business includes a plugins feature that you can use to interact with third-party services such as Jira and Salesforce. With the plugins feature, you can perform actions specific to that service (like creating a ticket) from within your Amazon Q Business web experience chat. For more information, see Plugins.

Quick prompts

The Amazon Q Business quick prompts feature helps with end user discoverability of the web experience chat features. Use this feature to prompt your end user to engage with their web experience chat in specific ways. For example, you can show the available configured plugins or inform users that they can choose to summarize their chat.

Response personalization

Response personalization is a Amazon Q Business feature that customizes chat responses to end users based on metadata associated with them—specifically address and job-related information—in your SSO instance. This feature enhances the relevance of responses by tailoring them to the user's specific context within the organization. To use response personalization effectively, you must have already added the necessary user information in your SSO instance. For more information, see Response settings.

Retriever

A retriever pulls data from an index in real time during a conversation. Amazon Q Business supports a native index retriever and also a Amazon Kendra index retriever.

Retrieval Augmented Generation

Retrieval Augmented Generation (RAG) is a natural language processing (NLP) technique. Using RAG, generative artificial intelligence (generative AI) is conditioned on specific documents that are retrieved from a dataset. Amazon Q Business has a built-in RAG system. A RAG model has the following two components:

- A *retrieval* component retrieves relevant documents for the user query.
- A *generation* component takes the query and the retrieved documents and then generates an answer to the query using a large language model.

Relevance tuning

You can choose to use document attributes to boost and tune the relevance of chat responses for end users from specific content. For example, if you have a document attribute associated document creation or updating date, you use these attributes to boost chat responses from more recently created or updated documents. For more information, see Relevance tuning.

Subscription tiers

Amazon Q Business offers multiple user subscription tiers and index types that can be combined to meet your organization's needs. User subscription tiers determine the features available to end users, with both Lite and Pro tier users having access to browser extensions. Index types include starter index and enterprise index, each with different capabilities and storage capacities. You can choose any combination of index types and user subscriptions for your Amazon Q Business application. For more information, see Amazon Q Business subscription tiers and index types.

> **Important**
>
> Amazon Q Business Pro tier subscriptions in Europe (Ireland) (eu-west-1) and Asia Pacific (Sydney) (ap-southeast-2) regions are available with a limited set of features.

Tags

Manage your Amazon Q Business applications and data sources by assigning tags or labels. You can use tags to categorize your Amazon Q Business resources in various ways. For example, categorize by purpose, owner, or application environment, or any combination. Each tag consists of a key and a value, both of which you define. For more information, see Tags.

Visual content extraction

When Amazon Q Business processes your input files from a data source, it uses advanced image understanding capabilities to extract semantic information and insights from images and other visuals. This feature makes visual information in your data sources queryable, allowing end users to find relevant information even when it's conveyed in embedded diagrams, charts, or technical illustrations. Visual content extraction provides additional context and nuance to the information in your data sources and builds a more complete knowledge base from your enterprise data. For more information, see Extracting semantic meaning from embedded visual content.

User store

User Store is an Amazon Q Business data source connector feature that streamlines user and group management across all the data sources attached to your application environment. For more information about how this feature works and implementation details, see Understanding User Store.

Web experience

An Amazon Q Business web experience is the chat interface that you create using your Amazon Q Business application environment. Then, your end users can chat with your organization's Amazon Q Business web experience. You can configure and customize your Amazon Q Business web experience using either the Amazon Q Business console or the Amazon Q Business API. For more information, see Customizing your web experience.

Amazon Q Business subscription tiers and index types

Amazon Q Business offers multiple index types and user subscription tiers. You can choose any combination of index types and user subscriptions for your Amazon Q Business application environment.

Topics

- Index types
- User subscription tiers
- Understanding user subscriptions
- Pricing

Index types

Amazon Q Business offers two types of indexes: starter index and enterprise index. Each index type has different capacity limits measured in index units, which determine the amount of data storage and processing capacity available for your index. For detailed information about index units and capacity, see Index capacity.

The following table outlines the features of both index types.

Starter index	Enterprise index
Ideal use case • Proof-of-concept or developer workloads	**Ideal use case** • Production workloads
Features • Runs in 1 Availability Zone (AZ) – See Availability Zones (data centers in AWS regions) • Includes up to 20,000 document capacity or 200 MB of total extracted text (whichever is reached first)* • Includes up to 100 hours of data source connector usage (time that it takes to scan and index new, updated, or deleted documents)	**Features** • Runs in 3 Availability Zone (AZ) – See Availability Zones (data centers in AWS regions) • Includes up to 20,000 document capacity or 200 MB of total extracted text (whichever is reached first)* • Includes up to 100 hours of data source connector usage (time that it takes to scan and index new, updated, or deleted documents) • Includes customer managed key encryption support

*For reference, 5 pages of text that contain approximately 500 words on each page is equivalent to 10 KB of total extracted text.

For detailed pricing information, including examples of charges for index capacity, subscribing and unsubscribing users to Amazon Q Business tiers, upgrading and downgrading Amazon Q Business tiers, and more, see Amazon Q Business Pricing.

User subscription tiers

Amazon Q Business offers two subscription tiers: the Amazon Q Business Lite Plan and the Amazon Q Business Pro Plan. The following table outlines the features of Amazon Q Business Pro and Amazon Q Business Lite.

Important

Amazon Q Business Pro tier subscriptions in Europe (Ireland) (eu-west-1) and Asia Pacific (Sydney) (ap-southeast-2) regions are available with a limited set of features.

Important

As of July 1, 2024, Amazon Q Apps only available to Amazon Q Business Pro users. Users with Lite subscriptions should upgrade to Amazon Q Business Pro.

Topics

- Amazon Q Business Lite users must upgrade to Amazon Q Business Pro to continue using Q Apps

Amazon Q Business Lite Plan	Amazon Q Business Pro Plan
Ideal use case • Optimized for enterprise-wide deployment to all employees (frontline and knowledge workers) • Allows end users to ask questions and receive permissions-aware responses from enterprise data sources with citations • Helps employees quickly get answers for use cases such as IT, HR, benefits help desks, and other Q&A chatbot use cases at a low cost **Features** • **Q&A on knowledge bases:** Users can ask questions and get answers from enterprise knowledge bases with citations.	**Ideal use case** • Best suited for knowledge workers and improves productivity across a wide range of tasks • Provides the full suite of Amazon Q Business capabilities • Includes access to Amazon Q Apps * for creating and sharing task automation applications • Includes access to integrations within third-party applications including Slack, Microsoft Teams, and browser extensions for Google Chrome, Mozilla Firefox, and Microsoft Edge • Includes access to custom plugins for actions like submitting time off requests and sending meeting invites through Amazon Q Business

Amazon Q Business Lite Plan	Amazon Q Business Pro Plan
• **Upload file to chat:** Users can upload documents into a chat session and interact with its contents. • **Permissions-aware responses:** Users only get answers from content that they have access to. • **Using web experience with single-sign on:** Users get access to a web experience user interface with support for single sign-on (IAM Identity Center). • **Browser extensions:** Users can access Amazon Q Business through browser extensions for Google Chrome, Mozilla Firefox, and Microsoft Edge. **Note:** Built-in and custom plugins are not available with the Lite Plan. Users must upgrade to the Pro Plan to access plugin functionality.	• Includes Amazon Q integration in Quick Pro for understanding data through executive summaries, context-aware Q&A, and interactive data stories **Features** • **Q&A on LLM knowledge:** Users can ask questions and get answers from the general knowledge that the LLM has. • **Q&A on knowledge bases:** Users can ask questions and get answers from enterprise knowledge bases with citations. • **Permissions-aware responses:** Users only get answers from content that they have access to. • **Using web experience with single-sign on:** Users get access to a web experience user interface with support for single sign-on (SSO). • **Content generation:** Users can send queries directly to the foundation model to generate content. • **Upload file to chat:** Users can upload documents into a chat session and interact with its contents. • **Amazon Q Apps:** Users can build and share their own purpose-built applications to automate tasks and improve productivity. • **Custom plugins:** Enable users to execute actions in third-party applications. • **Built-in plugins:** Access to pre-built integrations with third-party applications

Amazon Q Business Lite Plan	Amazon Q Business Pro Plan
	such as Salesforce, Jira, ServiceNow, and others. • **Amazon Q Business in Quicksight (Reader Pro):** Users can ask questions to explore data in natural language, view and interact with dashboards, and create compelling stories from insights. • **Chat orchestration:** automatically manage chat requests across configured plugins and data sources in your Amazon Q Business application. • **Integrations with third-party applications:** Users can access Amazon Q Business within third-party applications such as Slack and Microsoft Teams, and web browsers through browser extensions for Google Chrome, Mozilla Firefox, and Microsoft Edge.

For detailed pricing information, including examples of charges for index capacity, subscribing and unsubscribing users to Amazon Q Business tiers, upgrading and downgrading Amazon Q Business tiers, and more, see Amazon Q Business Pricing.

Amazon Q Business Lite users must upgrade to Amazon Q Business Pro to continue using Q Apps

As of July 1, 2024, Amazon Q Apps are available only to Amazon Q Business Pro users. Amazon Q Business Lite users will no longer be able to create, run, or view Q Apps. To access, Q Apps, Lite users must upgrade to Amazon Q Business Pro.

As of August 30, 2024, all Amazon Q Apps created by Lite users who did not upgrade their account to Amazon Q Business Pro have been deleted.

Understanding user subscriptions

User subscriptions are created per Amazon Q Business application or Quick account. Each admin can manage subscriptions for users for their specific Amazon Q Business application or Quick account.

For applications using IAM Identity Center, AWS will deduplicate subscriptions across all Amazon Q Business applications and Quick accounts, and charge each user only once for their highest subscription level. Note that deduplication will apply only if the Amazon Q Business applications and Quick accounts share the same IAM Identity Center instance.

Users subscribed to Amazon Q Business applications using Identity Federation through IAM (IAM Federation), will be charged once per OIDC or SAML IAM Identity Provider. For example, if a user is subscribed to five different Amazon Q Business applications all associated with the same IAM Identity Provider, that user will be charged once. However, if the Amazon Q Business applications are associated with five IAM Identity Providers, the user will be charged five times.

In scenarios where a user is subscribed to a mix of applications, the charging structure is as follows:

- For applications using IAM Identity Center, users will be charged once across all these applications that share the same IAM Identity Center instance.
- For applications using IAM Federation, users will be charged once per IAM Identity Provider.

User subscriptions are prorated when created or upgraded based on the number of days left in the calendar month. Any cancellations or downgrades are not prorated and apply starting in the next calendar month. The charges for user subscription starts only after first use by the user. After a user's first use, subscription charges will continue each month until the user's subscriptions have been removed.

For a consolidated view of all your user subscriptions see the Amazon Q subscriptions page. Subscriptions can only be viewed centrally and *not* be created or updated from the Amazon Q subscription management console.

Pricing

You are charged for user subscriptions to application environments and for index capacity. You can choose any combination of the following subscription tiers and indices for your application environment.

For detailed pricing information, including examples of charges for index capacity, subscribing and unsubscribing users to Amazon Q Business tiers, upgrading and downgrading Amazon Q Business tiers, and more, see Amazon Q Business Pricing.

Supported document formats in Amazon Q Business

When you add documents to an Amazon Q Business application environment (directly or through data source connectors) using the console or the API, Amazon Q Business extracts document content and internally parses these to optimize chat responses. During this ingestion, there are file size limits depending on the file type. Video files have a limit of up to 10 GB/10,240 MB. Audio files have a 2 GB/2,048 MB limit. PDF/Word/Powerpoint documents have a 500 MB limit. Excel and other supported file formats have a 50 MB limit. There are also limits to the amount of text extracted from these documents. CSV and Excel have a extracted text limit of 10MB, all other document formats have a limit of 30MB of extracted text.

When you upload documents directly into chat using the Upload files and chat feature, the size of each file you upload must be 10 MB or less, and 3.75 MB or less for images. The total parsed content for all files combined has to be under 665,000 characters.

For images, chat now supports direct uploads of JPEG, JPG, and PNG files. These images can be used for summarizing information and answering questions.

Additionally, if you're uploading Comma Separated Values (CSV) or Microsoft Excel (XLS and XLSX) documents directly into chat, Amazon Q Business performs best for tables with up to 4 columns and 10 rows. Files indexed by an Amazon Q Business data source connector or uploaded directly have no such restrictions.

When you directly add files to Amazon Q Business using the Using direct document upload or the Upload files and chat feature, it considers each file you add a document. When you connect Amazon Q Business to a data source, what Amazon Q Business considers—and crawls—as a document varies by connector.

Along with specific formats like PDF, Word, for example, each enterprise data source also has different entities that it considers documents. To learn about supported entity types for each data source, see What is a document?.

For some file types (indicated in the table below), Amazon Q Business can extract semantic information and insights from various types of images embedded in the documents. You can enable content extraction when you add or update a data connector, or when you import a file

directly. For more information see Extracting semantic meaning from embedded visual content with Amazon Q Business.

Topics

- Supported document types

Supported document types

The following table shows the document formats that Amazon Q Business supports.

> **Note**
>
> Provide a description of the file as metadata to improve retrieval accuracy. For more information, see Configuring metadata controls in Amazon Q Business.

Document format	How document is treated
Portable Document Format (PDF)	If you're using a data source connector, or directly uploading documents into your application, Amazon Q can use optical character recognition (OCR) to convert images of typed, handwritten, or printed text into machine-readable text. If enabled, Amazon Q Business can extract semantic information and insights from images and other visuals. The maximum number of pages per PDF for optical character recognition (OCR) or insight extraction from embedded visual elements is 3000 pages. If your PDF is more than 3000 pages, only plaintext is extracted. If you're directly uploading documents into chat, PDFs are converted to HTML, and only plaintext is extracted.

Document format	How document is treated
HyperText Markup Language (HTML)	HTML tags are filtered out to extract plaintext. Content must be between the main `HTML` start and closing tags (`<HTML>content</HTML>`).
Extensible Markup Language (XML)	XML tags are filtered out and plaintext is extracted.
Extensible Stylesheet Language Transformations (XSLT)	Tags are filtered out to extract plaintext.
Markdown (MD)	Content is extracted as plaintext with Markdown syntax retained.

Comma Separated Values (CSV)	Content is extracted as plaintext from each cell, with a single file treated as a single document result. You can improve answer accuracy on CSVs by providing a metadata file. Example:
	`"Attributes":{`
	`"description": "A description of your CSV table, a short paragraph providing details about what the use case is and insights you can derive from it.",`
	`"_document_title": "document title",`
	`"_file_type": "CSV"`
	`}`

Microsoft Excel (XLS and XLSX)	Content is extracted as plaintext from each cell, with a single file treated as a single document result.
JavaScript Object Notation (JSON)	Content is extracted as plaintext with JSON syntax retained.

Document format	How document is treated
Rich Text Format (RTF)	RTF syntax is filtered out to extract plaintext content.
Microsoft PowerPoint (PPT, PPTX)	By default, only plaintext content is extracted from PowerPoint slides for ingestion. If enabled, Amazon Q Business can extract semantic information and insights from images and other visuals. Otherwise, images and other content aren't extracted.
Microsoft Word (DOCX)	By default, only plaintext content is extracted from Word pages for ingestion. If enabled, Amazon Q Business can extract semantic information and insights from images and other visuals. Otherwise, images and other content aren't extracted.
Plain text (TXT)	All text in the text document is extracted.
Google Slides	By default, only plaintext content is extracted from Google Slides pages for ingestion. If enabled, Amazon Q Business can extract semantic information and insights from images and other visuals. Otherwise, images and other content aren't extracted.
Google Docs	By default, only plaintext content is extracted from Google Docs pages for ingestion. If enabled, Amazon Q Business can extract semantic information and insights from images and other visuals. Otherwise, images and other content aren't extracted.

Document attributes in Amazon Q Business

Every document has structural attributes—or metadata—attached to it. Document attributes can include information such as document title, document author, time created, time updated, and document type.

You can map document attributes to fields in your Amazon Q Business index. Once mapped to document attributes, these index fields can be used by admin to boost results from specific sources, or by end users to filter and scope their chat results to specific data.

> **Note**
>
> Filtering using document attributes in chat is only supported through the API. Boosting search results using document attributes is supported on both the console and the API.

You can also use document attributes to prepare your data for—and customize and control—end user chat. To learn more, see Filtering using metadata, Document enrichment in Amazon Q Business, Metadata controls, and Metadata boosting.

Topics

- Types of document attributes
- Mapped document attributes
- Document attribute data types

Types of document attributes

Amazon Q Business supports two types of document attributes: reserved or default, and custom.

Reserved or default document attributes are provided by Amazon Q Business to map commonly occurring document attributes to index fields. Custom attributes, on the other hand, can be used to map document attributes unique to your content to index fields.

Both reserved and custom document attributes can be used to customize end user chat experience.

Important

You can create and map up to 50 document attributes to index fields. Once created, you can't delete or rename any attributes.

The following section outlines the available document attributes.

Topics

- Reserved document attributes
- Custom document attributes

Reserved document attributes

Amazon Q Business offers the following reserved document attributes or index fields that you can map your metadata to:

- `_authors` – A list of one or more authors responsible for the content of the document.
- `_category` – A category that places a document in a specific group.
- `_created_at` – The date and time in ISO 8601 format that the document was created. For example, 2012-03-25T12:30:10+01:00 is the ISO 8601 date-time format for March 25, 2012 at 12:30 PM (plus 10 seconds) in Central European Time.
- `_data_source_id` – The identifier of the data source that contains the document.
- `_document_body` – The content of the document.
- `_document_id` – A unique identifier for the document.
- `_document_title` – The title of the document.
- `_file_type` – The file type of the document, such as .pdf or .docx.
- `_last_updated_at` – The date and time in ISO 8601 format that the document was last updated. For example, 2012-03-25T12:30:10+01:00 is the ISO 8601 date-time format for March 25, 2012 at 12:30 PM (plus 10 seconds) in Central European Time.
- `_source_uri` – The URI where the document is available. For example, the URI of the document on a company website.
- `_version` – An identifier for the specific version of a document.
- `_view_count` – The number of times that the document has been viewed.

- `_language_code (String)` – The code for a language that applies to the document. This defaults to English if you don't specify a language.
- `_data_source_type` – An **optional** type of data source that contains the document, specified as a text identifier (for example, "Amazon S3" or "WEBCRAWLERV2").

In addition to these default attributes, each Amazon Q Business data source connector also automatically creates specific reserved or default attributes based on commonly occurring metadata in the data source you're using. You can choose to map these to Amazon Q Business index fields when you configure a data source. You can't edit these default attributes.

Custom document attributes

You can create custom attributes based on your own enterprise data. You can map the custom attributes to index fields for a more tailored end user chat experience. For example, you can create a custom attribute called "Department" with the values of "HR", "Sales", and "Manufacturing" and map it an index field. Then, you can use these fields or attributes to allow your end users to filter their chat results to documents in the "HR" department, or restrict response generation to specific data stores.

You can also create and map custom document attributes based on uniquely occurring metadata in your data when you connect and configure a Amazon Q Business data source connector. If a document attribute in your data source doesn't have a default attribute mapping already available, or if you want to map additional document attributes to index fields, you can use these custom field mappings to specify how a data source attribute maps to an Amazon Q Business index field. You create and map custom document attributes to index fields by editing your data source after your application environment and retriever are created.

Mapped document attributes

When a document attribute—reserved or custom—is mapped to an index field, you can choose how the field will be used during chat. You can currently configure index fields to perform the following action:

- **Searchable** – Allows end users the ability to search data with the specified attributes.

Important

You can mark up to 30 index fields searchable.

Document attribute data types

Document attributes—reserved or custom—can only be the data types that are shown in the following table. Additionally, document attributes can be used to perform the operations outlined.

Data type	Searchable	Filterable	Boostable		
Date	Yes	Yes	Yes		
Number	Yes	Yes	Yes		
String	Yes	Yes	Yes		
String list	Yes	Yes	Yes		

Note

You can't change an index field type after it has been created.

For more information on filtering and boosting using document attributes, see Filtering using document-attributes and Boosting using document attributes.

Supported languages for Amazon Q Business

Amazon Q Business is optimized to respond in English. Amazon Q Business only indexes English language documents when you connect a Amazon Q Business data source or directly upload documents into your application. We recommend indexing only English language content.

Setting up for Amazon Q Business

Before you begin using Amazon Q Business for the first time, complete the following tasks.

Topics

- Initial AWS account setup
- (Optional) Install the AWS CLI
- (Optional) Set up the AWS SDKs
- Consider AWS Regions and endpoints
- Set up required permissions

Initial AWS account setup

Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call or text message and entering a verification code on the phone keypad.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to a user, and use only the root user to perform tasks that require root user access.

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to https://aws.amazon.com/ and choosing **My Account**.

Create a user with administrative access

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and create an administrative user so that you don't use the root user for everyday tasks.

Secure your AWS account root user

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

   For help signing in by using root user, see Signing in as the root user in the *AWS Sign-In User Guide*.

2. Turn on multi-factor authentication (MFA) for your root user.

   For instructions, see Enable a virtual MFA device for your AWS account root user (console) in the *IAM User Guide*.

Create a user with administrative access

1. Enable IAM Identity Center.

   For instructions, see Enabling AWS IAM Identity Center in the *AWS IAM Identity Center User Guide*.

2. In IAM Identity Center, grant administrative access to a user.

   For a tutorial about using the IAM Identity Center directory as your identity source, see Configure user access with the default IAM Identity Center directory in the *AWS IAM Identity Center User Guide*.

Sign in as the user with administrative access

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

  For help signing in using an IAM Identity Center user, see Signing in to the AWS access portal in the *AWS Sign-In User Guide*.

Assign access to additional users

1. In IAM Identity Center, create a permission set that follows the best practice of applying least-privilege permissions.

   For instructions, see Create a permission set in the *AWS IAM Identity Center User Guide*.

2. Assign users to a group, and then assign single sign-on access to the group.

   For instructions, see Add groups in the *AWS IAM Identity Center User Guide*.

(Optional) Install the AWS CLI

The AWS Command Line Interface (AWS CLI) is a unified developer tool for managing AWS services, including Amazon Q Business.

1. To install the AWS CLI, follow the instructions in Installing the AWS Command Line Interface in the *AWS Command Line Interface User Guide*.
2. To configure the AWS CLI and set up a profile to call the AWS CLI, follow the instructions in Configuring the AWS CLI in the *AWS Command Line Interface User Guide*.
3. To confirm that the AWS CLI profile is configured, run the following command:

   ```
   aws configure --profile default
   ```

   If your profile has been configured correctly, you will see output similar to the following:

   ```
   AWS Access Key ID [****************52FQ]:
   AWS Secret Access Key [****************xgyZ]:
   Default region name [us-west-2]:
   Default output format [json]:
   ```

4. To verify that the AWS CLI is configured for use with Amazon Q Business, run the following commands:

   ```
   aws qbusiness help
   ```

   If the AWS CLI is configured correctly, you will see a list of the supported AWS CLI commands for Amazon Q Business, Amazon Q Business runtime, and Amazon Q Business events.

(Optional) Set up the AWS SDKs

Download and install the AWS SDKs that you want to use. This guide provides examples for Python. For information about other AWS SDKs, see Tools for Amazon Web Services.

The package for the Python SDK is called *Boto3*.

Before you run the following Python commands, you must first download and install Python 3.6 or later for your operating system. Support for Python 3.5 and earlier is deprecated.

If you don't have pip included in your Python Scripts directory, you can download get-pip.py and store this in your Scripts directory. You can also set your Python directory as a Path or environment variable using a terminal program.

To install Python, complete the following steps:

```
# Install the latest Boto3 release via pip
pip install boto3

# You can install a specific version of Boto3 for compatibility reasons
# Install Boto3 version 1.0 specifically
pip install boto3==1.0.0

# Make sure Boto3 is no older than version 1.15.0
pip install boto3>=1.15.0

# Avoid versions of Boto3 newer than version 1.15.3
pip install boto3<=1.15.3
```

To use Boto3, you must set up authentication credentials for your AWS account using the IAM console.

Consider AWS Regions and endpoints

An *endpoint* is a URL that's the entry point for a web service. Each endpoint is associated with a specific AWS Region.

If you use a combination of the Amazon Q Business console, the AWS CLI, and the Amazon Q Business SDKs, pay attention to their default Regions. All Amazon Q Business components of a given application must be created in the same Region. Examples of a component include a retriever, an index, and a chat experience. To understand why this is important, see Considerations for choosing an AWS Region in the IAM Identity Center User Guide.

For regions and endpoints supported by Amazon Q Business, see Service quotas for Amazon Q Business.

Set up required permissions

If you use Amazon Q Business through the AWS Management Console, basic required permissions are added on your behalf.

To use Amazon Q Business as an IAM user on the AWS CLI, or AWS SDK, you must attach the following permissions to allow Amazon Q Business to create and manage resources on your behalf:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessFullAccessPermissions",
            "Effect": "Allow",
            "Action": "qbusiness:*",
            "Resource": "*"
        }
    ]
}
```

If you're using Q Apps, add the following permissions:

```
"qapps:*"
```

If you're using Q Apps, add the following permissions:

```
"quicksight:*"
```

If you're using a customer managed key, add the following permissions:

```
"kms:DescribeKey"
"kms:CreateGrant"
```

If you're using IAM Identity Center, add the following permissions:

```
"sso:CreateApplication",
"sso:PutApplicationAuthenticationMethod",
```

```
"sso:PutApplicationAccessScope",
"sso:PutApplicationGrant",
"sso:DeleteApplication",
"organizations:DescribeOrganization",
"sso-directory:DescribeGroup",
"sso-directory:DescribeUser",
"sso:DescribeApplication",
"sso:DescribeInstance"
```

To assign user subscriptions to applications, you must include permissions to call the necessary user subscription-related APIs. The subscription-related APIs give permission to create, update, cancel, and view all user subscriptions for an application. You can assign user subscriptions through both the Amazon Q Business console and programmatically using the AWS CLI or AWS SDKs.

To allow Amazon Q to assign user subscriptions, use the following role policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessSubscriptionPermissions",
            "Effect": "Allow",
            "Action": [
                "qbusiness:UpdateSubscription",
                "qbusiness:CreateSubscription",
                "qbusiness:CancelSubscription",
                "qbusiness:ListSubscriptions"
            ],
            "Resource": [
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id",
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id/subscription/subscription-id"
            ]
        },
        {
            "Sid": "QBusinessServicePermissions",
            "Effect": "Allow",
            "Action": [
                "user-subscriptions:UpdateClaim",
```

```
                "user-subscriptions:CreateClaim",
                "organizations:DescribeOrganization",
                "iam:CreateServiceLinkedRole",
                "sso-directory:DescribeGroup",
                "sso-directory:DescribeUser",
                "sso:DescribeApplication",
                "sso:DescribeInstance"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Grant permission to create data sources with ACLs disabled

By default, when Amazon Q administrators create data sources, ACLs are on. Some administrators may want to create data sources with ACLs disabled. You can grant them permission by attaching the IAM action `DisableAclOnDataSource` to their role or policy. With this permission, the administrator can create data sources with the ACL field disabled. If an administrator creates a data source with the ACL field set to enabled, they can't change the field to disabled. If they want to use a data source with ACLs disabled, they need to create a new data source.

We don't recommend disabling ACLs in production environments.

> **Warning**
>
> When ACLs are disabled for a data source, all documents ingested by the data source become accessible to all end users of the Amazon Q Business application.

You can check if data source connectors were created with ACLs disabled and whether Amazon Q administrators have the `DisableAclOnDataSource` IAM policy. To check ACLs on a data source, review `CreateDataSource` and `UpdateDataSource` event logs in CloudTrail. To check if administrators have been granted the `DisableAclOnDataSource`IAM action, review permissions in the IAM console.

As a best practice, we recommend you use an explicit deny on the `DisableAclOnDataSource`IAM action and that you only grant the `DisableAclOnDataSource` permission when requested by Amazon Q administrators.

> **Note**
>
> This feature is only available for use with the following connectors: ServiceNow Online, Confluence, SharePoint, Jira, Google Drive, OneDrive, Salesforce, Zendesk, GitHub, MS Teams, and Slack.

Example An example policy using `qbusiness:DisableAclOnDataSource`

The following is an example policy showing how to use `qbusiness:DisableAclOnDataSource`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ExplicitDenyACLDisable",
            "Effect": "Deny",
            "Action": [
                "qbusiness:DisableAclOnDataSource"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

For a complete list of IAM roles for Amazon Q Business, see IAM roles for Amazon Q Business.

IAM roles for Amazon Q Business

When you create an application or a web experience with Amazon Q Business, or connect a data source to it, Amazon Q Business needs access to the required AWS resources.

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create the Amazon Q Business resource. When you call an API operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role. The console displays roles that have the string **qbusiness** or **QBusiness** in the role name.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

The following topics provide details for the required policies. If you create IAM roles using the Amazon Q Business console, these policies are created on your behalf, unless otherwise noted.

Topics

- IAM role for an Amazon Q Business application
- IAM role for an Amazon Q Business web experience
- IAM role for Amazon Q Business data source connectors
- IAM role for Amazon Q Business plugins
- IAM roles for custom document enrichment in Amazon Q Business
- IAM role for an Amazon Kendra retriever

IAM role for an Amazon Q Business application

When you create an Amazon Q Business application, you must provide Amazon Q with an IAM role with permissions to write to an Amazon CloudWatch log and assign user subscriptions to applications. You must also provide a trust policy that allows Amazon Q to assume the role. The following are the policies that must be provided.

To allow Amazon Q to access a CloudWatch log and assign user subscriptions, use the following role policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "AmazonQApplicationPutMetricDataPermission",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/QBusiness"
                }
            }
        },
        {
            "Sid": "AmazonQApplicationDescribeLogGroupsPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AmazonQApplicationCreateLogGroupPermission",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:log-group:/aws/qbusiness/*"
            ]
        },
        {
            "Sid": "AmazonQApplicationLogStreamPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogStreams",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:log-group:/aws/qbusiness/
*:log-stream:*"
            ]
        }
    ]
```

```
}
```

To allow Amazon Q to assume a role, use the following trust policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonQApplicationPermission",
            "Effect": "Allow",
            "Principal": {
                "Service": "qbusiness.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/*"
                }
            }
        }
    ]
}
```

Amazon Q also supports using a service-linked role (`AWSServiceRoleForQBusiness`) for an Amazon Q application. The following is the service-linked role policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessPutMetricDataPermission",
```

```
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/QBusiness"
                }
            }
        },
        {
            "Sid": "QBusinessCreateLogGroupPermission",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/qbusiness/*"
            ]
        },
        {
            "Sid": "QBusinessDescribeLogGroupsPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "QBusinessLogStreamPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogStreams",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/qbusiness/*:log-stream:*"
            ]
        }
    ]
}
```

For more information on using service-linked roles for an Amazon Q application, see Using service-linked roles.

IAM role for an Amazon Q Business web experience

> **Note**
>
> If you are using permissions for Amazon Q Apps created prior to July 10, 2024, you must update your role with the new Amazon Q Apps permissions for your users to have access to use the permissions to view and specify approved data sources and other future features in Q Apps.

To allow Amazon Q to invoke the API operations required to integrate your application environment, deploy your chat web experience, use an external IdP, and use Amazon Q Apps you must use the following IAM policies.

Topics

- IAM role for an Amazon Q Business web experience using IAM Identity Center
- IAM role for an Amazon Q Business web experience using IAM Federation
- IAM permissions for using Amazon Q Apps

IAM role for an Amazon Q Business web experience using IAM Identity Center

> **Important**
>
> This page only applies to Amazon Q Business web experiences connected to IAM Identity Center-integrated Amazon Q Business applications.

Policy history

- **Latest policy update:** — December 3, 2024

The following table list and describes the changes to this policy over time.

Change	Description	Date
Amazon Q Business now supports deleting attachments	To enable delete attachments support on chats, modify your *Web experience IAM role* by adding the permission `qbusiness:DeleteAttachment`. The scoping for this new permission should be similar to other `qbusiness:` conversation permissions. With this change, users can remove attached files in conversations.	2/27/2025
Amazon Q Business plugin actions support	To allow Amazon Q Business to list plugin actions and to allow end users to discover plugins in their web experience, modify the existing *Web experience IAM role* by adding the following permissions: `qbusiness:ListPluginActions`, `qbusiness:ListPluginTypeMetadata`, and `qbusiness:ListPluginTypeActions`. The scoping for this new permission should be similar to other `qbusiness:` conversation permissions. With this change, Amazon Q Business can list plugin actions and web experience users can discover plugins	12/03/2024

Change	Description	Date
	in their web experience. For more information, see Prerequisites for configuring Amazon Q Business built-in plugins.	
Amazon Quick plugin support	To allow the Quick plugin to include visuals from Amazon Quick, modify the existing *Web experience IAM role* to add permission for `quicksight:GenerateEmbedUrlForRegisteredUserWithIdentity` . With this change, web experience users can view visuals from Quick. For more information about the Quick plugin, see Using the Quick plugin to get insights from structured data.	12/03/2024

Change	Description	Date
Embedded visual content support	To enable extracting semantic meaning from embedded visual content, modify the existing *Web experience IAM role* by adding the permissio n `qbusiness:GetMedia` . The scoping for this new permission should be similar to other `qbusiness:` conversation permissions. With this change, if you enable content extraction for a data source, web experienc e users can ask questions and get answers related to the images. When an end user asks a question, Amazon Q Business retrieves relevant answers from the text and the images. Answers include the images and links for the documents that contain them. For more informati on, see Extracting semantic meaning from embedded visual content with Amazon Q Business.	12/01/2024

Change	Description	Date
Recent files support	To enable recent files support on web experiences, modify the existing *Web experienc e IAM role* by adding the permission `qbusiness :ListAttachments` . The scoping for this new permission should be similar to other `qbusiness:` conversation permissions. With this change, users can find and reuse any recently attached files in new conversations without uploading the files again. Additionally, users can now drag and drop files they want to upload directly into any conversation inside their Amazon Q web experience.	11/21/2024

Note

To find the IAM role ARN for your web experience you can go to **Amazon Q Business** → **Applications** → ***choose your application*** **Name** → **Web experience settings** in the Amazon Q Business console.

The following section lists the IAM policies required to allow you to invoke the API operations required to integrate your application environment with IAM Identity Center.

To allow an Amazon Q Business web experience to invoke the API operations required to integrate your application environment and deploy your web experience with an IAM Identity Center instance, use the following policy:

Note

To make use of the Clickable URL feature, add the following permissions to the IAM role for your Amazon Q web experience.

```
{
    "Sid": "QBusinessGetDocumentContentPermission",
    "Effect": "Allow",
    "Action": ["qbusiness:GetDocumentContent"],
    "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/*"
    ]
}
```

To allow Amazon Q to assume this role, use the following trust policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessTrustPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "application.qbusiness.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
```

```
                },
                "ArnEquals": {
                    "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
                }
            }
        }
    ]
}
```

IAM role for an Amazon Q Business web experience using IAM Federation

> **Important**
>
> This page only applies to Amazon Q Business web experiences connected to IAM Federated Amazon Q Business applications.

Policy history

- **Latest policy update:** — December 3, 2024

The following table list and describes the changes to this policy over time.

Change	Description	Date
Amazon Q Business now supports deleting attachments	To enable delete attachments support on chats, modify your *Web experience IAM role* by adding the permission `qbusiness:DeleteAttachment` . The scoping for this new permission should be similar to other `qbusiness:` conversation permissions.	2/27/2025

Change	Description	Date
	With this change, users can remove attached files in conversations.	
Amazon Q Business plugin actions support	To allow Amazon Q Business to list plugin actions and to allow end users to discover plugins in their web experienc e, modify the existing *Web experience IAM role* by adding the following permissions: `qbusiness:ListPlug inActions` , `qbusiness :ListPluginTypeMet adata` , and `qbusiness :ListPluginTypeAct ions` . The scoping for this new permission should be similar to other `qbusiness :` conversation permissions. With this change, Amazon Q Business can list plugin actions and web experienc e users can discover plugins in their web experience. For more information, see Prerequisites for configuring Amazon Q Business built-in plugins.	12/03/2024

Change	Description	Date
Embedded visual content support	To enable extracting semantic meaning from embedded visual content, modify the existing *Web experience IAM role* by adding the permissio n `qbusiness:GetMedia` . The scoping for this new permission should be similar to other `qbusiness:` conversation permissions. With this change, if you enable content extraction for a data source, web experienc e users can ask questions and get answers related to the images. When an end user asks a question, Amazon Q Business retrieves relevant answers from the text and the images. Answers include the images and links for the documents that contain them. For more informati on, see Extracting semantic meaning from embedded visual content with Amazon Q Business.	12/01/2024

Change	Description	Date
Recent files support	To enable recent files support on web experiences, modify the existing *Web experienc e IAM role* by adding the permission `qbusiness :ListAttachments` . The scoping for this new permission should be similar to other `qbusiness:` conversation permissions. With this change, users can find and reuse any recently attached files in new conversations without uploading the files again. Additionally, users can now drag and drop files they want to upload directly into any conversation inside their Amazon Q web experience.	11/21/2024

Note

To find the IAM role ARN for your web experience you can go to **Amazon Q Business** → **Applications** → ***choose your application*** **Name** → **Web experience settings** in the Amazon Q Business console.

The following IAM policies allow you to invoke the API operations required for an application environment using Identity Federation through IAM (IAM Federation) to manage user access or deploy a web experience using an external IdP.

Note

You must create and update an IAM policy for your Amazon Q Business application (both console and API) before you begin creating it. Amazon Q Business doesn't auto-create IAM roles for your IAM Federation application if you use the console.

To allow an Amazon Q Business web experience to invoke the API operations required to integrate your application environment and deploy your web experience with an AWS Identity and Access Management instance, use the following policy:

Note

To make use of the Clickable URL feature, add the following permissions to the IAM role for your Amazon Q web experience.

```
{
    "Sid": "QBusinessGetDocumentContentPermission",
    "Effect": "Allow",
    "Action": ["qbusiness:GetDocumentContent"],
    "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/*"
    ]
}
```

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessConversationPermissions",
```

```
            "Effect": "Allow",
            "Action": [
                "qbusiness:Chat",
                "qbusiness:ChatSync",
                "qbusiness:ListMessages",
                "qbusiness:ListConversations",
                "qbusiness:PutFeedback",
                "qbusiness:DeleteConversation",
                "qbusiness:GetWebExperience",
                "qbusiness:GetApplication",
                "qbusiness:ListPlugins",
                "qbusiness:GetChatControlsConfiguration",
                "qbusiness:ListRetrievers",
                "qbusiness:ListPluginActions",
                "qbusiness:ListAttachments",
                "qbusiness:GetMedia",
                "qbusiness:DeleteAttachment"
            ],
            "Resource": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
        },
        {
            "Sid": "QBusinessPluginDiscoveryPermissions",
            "Effect": "Allow",
            "Action": [
                "qbusiness:ListPluginTypeMetadata",
                "qbusiness:ListPluginTypeActions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "QBusinessRetrieverPermission",
            "Effect": "Allow",
            "Action": [
                "qbusiness:GetRetriever"
            ],
            "Resource": [
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id",
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id/retriever/*"
            ]
        },
        {
```

```
            "Sid": "QBusinessAutoSubscriptionPermission",
            "Effect": "Allow",
            "Action": [
                "user-subscriptions:CreateClaim"
            ],
            "Condition": {
                "Bool": {
                    "user-subscriptions:CreateForSelf": "true"
                },
                "StringEquals": {
                    "aws:CalledViaLast": "qbusiness.amazonaws.com"
                }
            },
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "QBusinessKMSDecryptPermissions",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/key-id"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "qbusiness.us-east-1.amazonaws.com",
                        "qapps.us-east-1.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "QAppsResourceAgnosticPermissions",
            "Effect": "Allow",
            "Action": [
                "qapps:CreateQApp",
                "qapps:PredictQApp",
                "qapps:PredictProblemStatementFromConversation",
                "qapps:PredictQAppFromProblemStatement",
                "qapps:ListQApps",
```

```
                "qapps:ListLibraryItems",
                "qapps:CreateSubscriptionToken"
            ],
            "Resource": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
        },
        {
            "Sid": "QAppsAppUniversalPermissions",
            "Effect": "Allow",
            "Action": [
                "qapps:DisassociateQAppFromUser"
            ],
            "Resource": "arn:aws:qapps:us-
east-1:111122223333:application/application-id/qapp/*"
        },
        {
            "Sid": "QAppsAppOwnerPermissions",
            "Effect": "Allow",
            "Action": [
                "qapps:GetQApp",
                "qapps:CopyQApp",
                "qapps:UpdateQApp",
                "qapps:DeleteQApp",
                "qapps:ImportDocument",
                "qapps:CreateLibraryItem",
                "qapps:UpdateLibraryItem",
                "qapps:StartQAppSession"
            ],
            "Resource": "arn:aws:qapps:us-
east-1:111122223333:application/application-id/qapp/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "qapps:UserIsAppOwner": "true"
                }
            }
        },
        {
            "Sid": "QAppsPublishedAppPermissions",
            "Effect": "Allow",
            "Action": [
                "qapps:GetQApp",
                "qapps:CopyQApp",
                "qapps:AssociateQAppWithUser",
                "qapps:GetLibraryItem",
```

```
                "qapps:CreateLibraryItemReview",
                "qapps:AssociateLibraryItemReview",
                "qapps:DisassociateLibraryItemReview",
                "qapps:StartQAppSession"
            ],
            "Resource": "arn:aws:qapps:us-
east-1:111122223333:application/application-id/qapp/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "qapps:AppIsPublished": "true"
                }
            }
        },
        {
            "Sid": "QAppsAppSessionModeratorPermissions",
            "Effect": "Allow",
            "Action": [
                "qapps:ImportDocument",
                "qapps:GetQAppSession",
                "qapps:GetQAppSessionMetadata",
                "qapps:UpdateQAppSession",
                "qapps:UpdateQAppSessionMetadata",
                "qapps:StopQAppSession"
            ],
            "Resource": "arn:aws:qapps:us-
east-1:111122223333:application/application-id/qapp/*/session/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "qapps:UserIsSessionModerator": "true"
                }
            }
        },
        {
            "Sid": "QAppsSharedAppSessionPermissions",
            "Effect": "Allow",
            "Action": [
                "qapps:ImportDocument",
                "qapps:GetQAppSession",
                "qapps:GetQAppSessionMetadata",
                "qapps:UpdateQAppSession"
            ],
            "Resource": "arn:aws:qapps:us-
east-1:111122223333:application/application-id/qapp/*/session/*",
            "Condition": {
```

```
                "StringEqualsIgnoreCase": {
                    "qapps:SessionIsShared": "true"
                }
            }
        }
    ]
}
```

To allow Amazon Q to assume this role for a web experience using SAML-compliant identity provider for user management, use the following trust policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": "sts:AssumeRoleWithSAML",
            "Sid": "SAMLAssumeRoleAccess",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "SAML:aud": "https://q-web-experience-domain/saml"
                }
            },
            "Principal": {
                "Federated": "arn:aws:iam::111122223333:saml-provider/
[[saml_provider]]"
            }
        },
        {
            "Action": "sts:TagSession",
            "Sid": "SAMLTagSessionAccess",
            "Effect": "Allow",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/Email": "*"
                }
            },
            "Principal": {
```

```
                "Federated": "arn:aws:iam::111122223333:saml-provider/
[[saml_provider]]"
            }
        }
    ]
}
```

To allow Amazon Q to assume this role for a web experience using an OIDC-compliant identity provider for user management, use the following trust policy:

To allow an Amazon Q Business web experience to access AWS KMS to decrypt an OIDC client secret stored in Secrets Manager for an OIDC-based identity provider:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:111122223333:secret:secret-id"
            ]
        },
        {
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/key-id"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
```

```
                    ]
                }
            }
        }
    ]
}
```

To allow Amazon Q to assume the role to decrypt an OIDC client secret stored in Secrets Manager, use the following trust policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
            "Effect": "Allow",
            "Principal": {
                "Service": "application.qbusiness.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
                }
            }
        }
    ]
}
```

IAM permissions for using Amazon Q Apps

If the users of your deployed web experience want to create lightweight, purpose-built Amazon Q Apps within your broader Amazon Q Business application environment, you must include the following policy permissions.

Note

This Amazon Q Apps IAM policy released on July 10, 2024 supports the ability for users to view and specify approved *data sources* at the card-level and use other future features. To use these features, you must update all roles for Amazon Q Apps that have been created prior to this date with this new policy.

Change	Description	Date
Deprecated some IAM actions related to file upload	The `qapps:ImportDocumentToQApp` , `qapps:ImportDocumentToQAppSession` , and `qapps:CreatePresignedUrl` IAM actions are deprecated. The `qapps:ImportDocument` action now serves as the single file upload action.	05/22/2025
Added Permission to `CreatePresignedUrl`	This new API allows users to leverage the improved file limits in Amazon Q Apps. You can now upload files with size up to 10MB (per file card).	11/22/2024
Added Permissions to `DescribeQAppPermissions` and `UpdateQAppPermissions`	These new APIs allows users privately share Amazon Q Apps to leverage the improved file limits in Amazon Q Apps. You can now upload files with size up to 10MB (per file card).	11/22/2024
Added permissions related to management of persistent sessions.	These new APIs allows users to start, manage and terminate long running	11/22/2024

Change	Description	Date
	collaborative data collection sessions to leverage the improved file limits in Amazon Q Apps. You can now upload files with size up to 10MB (per file card).	

Topics

- Capabilities available with Amazon Q Apps
- IAM permissions for users to view and specify approved data sources in Amazon Q Apps

If you want to use Amazon Q Apps, your web experience IAM role needs the following additional permissions:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QAppsResourceAgnosticPermissions",
            "Effect": "Allow",
            "Action": [
                "qapps:CreateQApp",
                "qapps:PredictQApp",
                "qapps:PredictProblemStatementFromConversation",
                "qapps:PredictQAppFromProblemStatement",
                "qapps:ListQApps",
                "qapps:ListLibraryItems",
                "qapps:CreateSubscriptionToken"
            ],
            "Resource": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
        },
        {
            "Sid": "QAppsAppUniversalPermissions",
            "Effect": "Allow",
```

```
            "Action": [
                "qapps:DisassociateQAppFromUser"
            ],
            "Resource": "arn:aws:qapps:us-
east-1:111122223333:application/application-id/qapp/*"
        },
        {
            "Sid": "QAppsAppOwnerPermissions",
            "Effect": "Allow",
            "Action": [
                "qapps:GetQApp",
                "qapps:CopyQApp",
                "qapps:UpdateQApp",
                "qapps:DeleteQApp",
                "qapps:ImportDocument",
                "qapps:CreateLibraryItem",
                "qapps:UpdateLibraryItem",
                "qapps:StartQAppSession",
                "qapps:DescribeQAppPermissions",
                "qapps:UpdateQAppPermissions"
            ],
            "Resource": "arn:aws:qapps:us-
east-1:111122223333:application/application-id/qapp/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "qapps:UserIsAppOwner": "true"
                }
            }
        },
        {
            "Sid": "QAppsPublishedAppPermissions",
            "Effect": "Allow",
            "Action": [
                "qapps:GetQApp",
                "qapps:CopyQApp",
                "qapps:AssociateQAppWithUser",
                "qapps:GetLibraryItem",
                "qapps:CreateLibraryItemReview",
                "qapps:AssociateLibraryItemReview",
                "qapps:DisassociateLibraryItemReview",
                "qapps:StartQAppSession",
                "qapps:DescribeQAppPermissions"
            ],
```

```
            "Resource": "arn:aws:qapps:us-
east-1:111122223333:application/application-id/qapp/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "qapps:AppIsPublished": "true"
                }
            }
        },
        {
            "Sid": "QAppsAppSessionModeratorPermissions",
            "Effect": "Allow",
            "Action": [
                "qapps:ImportDocument",
                "qapps:GetQAppSession",
                "qapps:GetQAppSessionMetadata",
                "qapps:UpdateQAppSession",
                "qapps:UpdateQAppSessionMetadata",
                "qapps:StopQAppSession",
                "qapps:ListQAppSessionData",
                "qapps:ExportQAppSessionData"
            ],
            "Resource": "arn:aws:qapps:us-
east-1:111122223333:application/application-id/qapp/*/session/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "qapps:UserIsSessionModerator": "true"
                }
            }
        },
        {
            "Sid": "QAppsSharedAppSessionPermissions",
            "Effect": "Allow",
            "Action": [
                "qapps:ImportDocument",
                "qapps:GetQAppSession",
                "qapps:GetQAppSessionMetadata",
                "qapps:UpdateQAppSession",
                "qapps:ListQAppSessionData"
            ],
            "Resource": "arn:aws:qapps:us-
east-1:111122223333:application/application-id/qapp/*/session/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "qapps:SessionIsShared": "true"
```

```
                }
            }
        }
    ]
}
```

Capabilities available with Amazon Q Apps

The Amazon Q Apps IAM policy allows your web experience users permissions to do the following:

- **Amazon Q Apps capabilities:**
  - Create a Q App (API)
  - Get the status and other information on a Q App (API)
  - Update a Q App (API)
  - List all created Q Apps (API)
  - Delete a Q App (API)
  - Start a Q App run (session) (API)
  - Stop a Q App run (session) (API)
  - Upload files to a Q App run (session) (API)
  - Converts a conversation into a (*text string*) problem statement (API)
  - Convert a problem statement into a proposed Q App (API)
- **Amazon Q Apps library capabilities:**
  - Publish a Q App by adding items to your Q Apps library (API)
  - Get the status and other information on a Q App (item) in your Q Apps library (API)
  - Update a published Q App (item) in your Q Apps library (API)
  - List all Q Apps (items) from your Q Apps library (API)
  - Delete a Q App (item) from your Q Apps library (API)
  - Like (rate) a Q App item from your Q Apps library (API)

IAM permissions for users to view and specify approved data sources in Amazon Q Apps

(Optional) You must add the following permissions to the Amazon Q Apps policy to allow Q Apps users to view and specify approved data sources in their app.

Note

If you are using permissions for Amazon Q Apps created prior to July 10, 2024, you must update your role with the new Amazon Q Apps permissions for your users to have access to use the permissions to view and specify approved data sources and other future features in Q Apps.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessIndexPermission",
            "Effect": "Allow",
            "Action": [
                "qbusiness:ListIndices"
            ],
            "Resource": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
        },
        {
            "Sid": "QBusinessDataSourcePermission",
            "Effect": "Allow",
            "Action": [
                "qbusiness:ListDataSources"
            ],
            "Resource": [
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id",
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id/index/*"
            ]
        }
    ]
}
```

Note

If any of these permissions are removed, then you run the risk of your web experience users not being able to create and run their own Q Apps properly.

IAM role for Amazon Q Business data source connectors

You can use either the Amazon Q Business console or the CreateDataSource API operation to connect your data source. However, you must first provide Amazon Q Business with an IAM role that has permissions to access the data source resources.

If you use the console, you can either create an IAM role when you connect your data source to Amazon Q Business or use an existing role. If you use the `CreateDataSource` API operation, you must provide the Amazon Resource Name (ARN) of an existing IAM role.

The specific permissions required depend on the data source. At a minimum, your IAM role must include the following:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` API operations in order to ingest documents.
- Permission to access the User Store APIs needed to ingest access control and identity information from documents.

Topics

- IAM role for Amazon Q Business data source connectors
- IAM role for Amazon S3 data sources

IAM role for Amazon Q Business data source connectors

When you use an Amazon Q Business data source, you require the following permissions, depending on your use case.

To allow Amazon Q Business to connect to your data source, use the following least-permissions role policy:

Note

This policy assumes your data source doesn't use any authentication.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id",
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id/index/index-id"
            ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id",
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id/index/index-id",
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id/index/index-id/data-source/*"
            ]
```

```
        }
    ]
}
```

To allow Amazon Q Business to assume a role, you must also use the following trust policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
            "Effect": "Allow",
            "Principal": {
                "Service": "qbusiness.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
                }
            }
        }
    ]
}
```

If your data source uses authentication, you must add the following policy to your IAM role to allow Amazon Q Business to access your AWS Secrets Manager secret:

```
{
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
```

```
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        }
```

If you are using an Amazon VPC, you must add the following VPC access permissions to your policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:111122223333:subnet/[[subnet_ids]]",
                "arn:aws:ec2:us-east-1:111122223333:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_111122223333_application-id_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
```

```
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
"qbusiness_111122223333_application-id_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

If your Secrets Manager secret is encrypted, you must add permissions for AWS KMS key to decrypt the username and password secret stored by Secrets Manager:

```
{
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
    ],
    "Condition": {
        "StringLike": {
            "kms:ViaService": [
                "s3.*.amazonaws.com"
            ]
        }
    }

}
```

If your Amazon Q Business data source connector needs access to an object stored in an Amazon S3 bucket (such as an SSL certificate), you must add the following permissions to your IAM role:

> **Note**
>
> Check that the file path to the object in your Amazon S3 bucket is of the following format: *s3://BucketName/FolderName/FileName.extension*.

```
{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        }
```

IAM role for Amazon S3 data sources

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q Business resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role while creating your data source.

> **Note**
>
> To learn how to create an IAM role, see Create a role to delegate permissions to an AWS service.

When you use an Amazon S3 bucket as a data source, you must provide a role that has permissions to:

- Access your Amazon S3 bucket.
- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` API operations in order to ingest documents.
- Access the Principal Store APIs needed to ingest access control and identity information from documents.

To allow Amazon Q to use an Amazon S3 bucket as a data source, use the following role policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAmazonQToGetObjectfromS3",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToListS3Buckets",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
```

```
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id",
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id/index/index-id"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCallPrincipalMappingAPIs",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id",
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id/index/index-id",
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id/index/index-id/data-source/*"
            ]
        }
    ]
}
```

If the documents in the Amazon S3 bucket are encrypted, you must provide the following permissions to use the AWS KMS key to decrypt the documents:

```
{
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
```

```
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    }
```

If you are using an Amazon VPC, you must add the following VPC access permissions to your policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAmazonQToGetObjectfromS3",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToListS3Buckets",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
```

```
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id",
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id/index/index-id"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCallPrincipalMappingAPIs",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id",
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id/index/index-id",
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id/index/index-id/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteENI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
```

```
                "arn:aws:ec2:us-east-1:111122223333:subnet/[[subnet_ids]]",
                "arn:aws:ec2:us-east-1:111122223333:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateDeleteENI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_111122223333_application-id_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
```

```
            "Resource": "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_111122223333_application-id_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToConnectToVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
            "Effect": "Allow",
            "Principal": {
                "Service": "qbusiness.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
```

```
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
                }
            }
        }
    ]
}
```

IAM role for Amazon Q Business plugins

To successfully connect Amazon Q Business to a plugin, you need to give Amazon Q Business the following permissions using a service access role:

- Permission to access your Secrets Manager secret to get the credentials you use to log in to the third party service instance you are creating a plugin for.
- **(Optional)** Permission to access the customer managed AWS KMS key used to encrypt the content of your Secrets Manager secret.

Amazon Q Business assumes this role to access your third party service instance credentials.

If you use the console and choose to create a new IAM role, Amazon Q creates the IAM role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your secret contains the following permissions.

> **Important**
>
> If you're changing response settings for an Amazon Q Business application created and deployed before 16 April, 2024, you need to update your web experience service role. For information on service role permissions needed, see IAM role for an Amazon Q Business web experience. For information on how to update your web experience service role, see Updating a web experience.

The following is the service access IAM role required:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowQBusinessToGetSecretValue",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:111122223333:secret:
[[secret_id]]"
            ]
        }
    ]
}
```

To allow Amazon Q Business to assume a role, use the following trust policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessApplicationTrustPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "qbusiness.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
                }
```

```
            }
        }
    ]
}
```

IAM roles for custom document enrichment in Amazon Q Business

Custom document enrichment (CDE) is an Amazon Q Business feature that you can use to manipulate your document content and document attributes. When you use the Lambda functions for CDE, you need an IAM role for the following:

- A role for `PreExtractionHookConfiguration` with permissions to run `PreExtractionHookConfiguration` and to access the Amazon S3 bucket when you use `PreExtractionHookConfiguration`.
- A role for `PostExtractionHookConfiguration` with permissions to run `PreExtractionHookConfiguration` and to access the Amazon S3 bucket when you use `PostExtractionHookConfiguration`.

> **Important**
>
> IAM roles for Custom Document Enrichmmnt (CDE) Lambda functions should belong to the same account as the account using BatchPutDocument API operation or the CreateDataSource operation to configure CDE.

Both AWS Identity and Access Management (IAM) roles must have the permissions to:

- Run `PreExtractionHookConfiguration` and/or `PostExtractionHookConfiguration`. To apply advanced alterations of your document metadata and content during the ingestion process, configure a Lambda function for `PreExtractionHookConfiguration` and/or `PostExtractionHookConfiguration`.
- (Optional) If you choose to activate Server Side Encryption for your Amazon S3 bucket, you must provide permissions to use the AWS KMS key customer to encrypt and decrypt the objects stored in your Amazon S3 bucket.

A role policy to allow Amazon Q to run `PreExtractionHookConfiguration` with encryption for your Amazon S3 bucket.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Effect": "Allow",
            "Sid": "S3GetObjectPermissions"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ],
            "Effect": "Allow",
            "Sid": "S3ListBucketPermissions"
        },
        {
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/key-id"
            ],
            "Effect": "Allow",
            "Sid": "KMSPermissions"
        },
        {
            "Action": [
```

```
                "lambda:InvokeFunction"
            ],
            "Resource": "arn:aws:lambda:us-east-1:111122223333:function:pre-
extraction-lambda-function",
            "Effect": "Allow",
            "Sid": "LambdaPermissions"
        }
    ]
}
```

An role policy to allow Amazon Q to run `PreExtractionHookConfiguration` without encryption.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Effect": "Allow",
            "Sid": "S3GetObjectPermissions"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name"
            ],
            "Effect": "Allow",
            "Sid": "S3ListBucketPermissions"
        },
        {
```

```
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": "arn:aws:lambda:us-east-1:111122223333:function:pre-
extraction-lambda-function",
            "Effect": "Allow",
            "Sid": "LambdaPermissions"
        }
    ]
}
```

A role policy to allow Amazon Q to run `PostExtractionHookConfiguration` with encryption for your Amazon S3 bucket.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Effect": "Allow",
            "Sid": "S3GetObjectPermissions"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name"
            ],
            "Effect": "Allow",
            "Sid": "S3ListBucketPermissions"
        },
```

```
        {
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/key-id"
            ],
            "Effect": "Allow",
            "Sid": "KMSPermissions"
        },
        {
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": "arn:aws:lambda:us-east-1:111122223333:function:post-
extraction-lambda-function",
            "Effect": "Allow",
            "Sid": "LambdaPermissions"
        }
    ]
}
```

An role policy to allow Amazon Q to run `PostExtractionHookConfiguration` without encryption.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Effect": "Allow",
```

```
            "Sid": "S3GetObjectPermissions"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name"
            ],
            "Effect": "Allow",
            "Sid": "S3ListBucketPermissions"
        },
        {
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": "arn:aws:lambda:us-east-1:111122223333:function:post-
extraction-lambda-function",
            "Effect": "Allow",
            "Sid": "LambdaPermissions"
        }
    ]
}
```

We recommend that you include `aws:sourceAccount` and `aws:sourceArn` in the trust policy. Their inclusion limits permissions and securely checks if `aws:sourceAccount` and `aws:sourceArn` are the same values as provided in the IAM role policy for the `sts:AssumeRole` action. This approach prevents unauthorized entities from accessing your IAM roles and their permissions. For more information, see confused deputy problem in the *IAM User Guide*.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Sid": "QBusinessTrustPolicy",
            "Effect": "Allow",
            "Condition": {
                "StringLike": {
```

```
                    "aws:SourceArn": "arn:aws:qbusiness:your-
region:123456789012:application/<application-id>/index/<index-id>"
                },
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                }
            },
            "Principal": {
                "Service": [
                    "qbusiness.amazonaws.com"
                ]
            }
        }
    ]
}
```

IAM role for an Amazon Kendra retriever

When you use an Amazon Kendra index as a retriever, you must provide Amazon Q Business with an IAM role with permissions to access Amazon Kendra. You must also provide a trust policy that allows Amazon Q to assume the role. The following are the policies that must be provided.

To allow Amazon Q to access your Amazon Kendra index, use the following policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "KendraRetrieveAccess",
            "Effect": "Allow",
            "Action": [
                "kendra:Retrieve",
                "kendra:DescribeIndex"
            ],
            "Resource": "arn:aws:kendra:us-east-1:111122223333:index/example-
index-id"
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonQKendraAccessPermission",
            "Effect": "Allow",
            "Principal": {
                "Service": "qbusiness.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnEquals": {
                    "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
                }
            }
        }
    ]
}
```

Configuring an Amazon Q Business application using AWS IAM Identity Center

As the first step towards creating a generative artificial intelligence (AI) assistant, you configure an application environment, and grant end user access to users to interact with an application environment using AWS IAM Identity Center for user management. Then you provision subscriptions for your IAM Identity Center users and groups.

Your authorized users interact with your application environment through the web experience. You share the endpoint URL of your web experience with your users, who open the URL and are authenticated before they can start chatting. The endpoint URL can be found in your web experience settings when selecting your application environment in the console.

This section guides you through the process of creating and configuring an Amazon Q Business application environment. To create an application environment, you can use the Amazon Q Business console, the AWS Command Line Interface (AWS CLI), and Amazon Q Business API operations.

As a prerequisite, make sure that you complete the setting up tasks and go through the configuring an IAM Identity Center instance section. If you're using the AWS CLI or the API, make sure that you've created the required IAM roles.

After you finish creating your application environment, you can customize and preview the web experience that it will power.

> **Note**
>
> Response generation from large language model (LLM) knowledge is enabled by default for your application.

Topics

- Configuring an IAM Identity Center instance for an Amazon Q Business application
- Creating an Amazon Q Business application environment
- Migrating an Amazon Q Business direct SAML 2.0 application to IAM Identity Center
- Making authenticated Amazon Q Business API calls using IAM Identity Center

- Managing Amazon Q Business application resources

Configuring an IAM Identity Center instance for an Amazon Q Business application

Amazon Q Business integrates with IAM Identity Center to enable managing end user access to your Amazon Q Business application. IAM Identity Center is the recommended method for managing human access to AWS resources. We recommend enabling and pre-configuring an IAM Identity Center instance before creating your Amazon Q Business application.

Topics

- Prerequisites
- Understanding types of IAM Identity Center instances
- Creating a same-region integration
- Creating a cross-region integration

Prerequisites

Before you create an Amazon Q Business application, make sure you complete the following prerequisites:

- Enable an IAM Identity Center instance and connect the identity source for your Amazon Q Business application environment in IAM Identity Center. Amazon Q Business supports both organization and account level IAM Identity Center instances.

  > **Note**
  >
  > To minimize latency, we recommend using an IAM Identity Center instance created in the same region as your Amazon Q Business application. However, you can also use an IAM Identity Center instance created in an AWS region not yet supported by Amazon Q Business. For more information, see Creating a cross-region IAM Identity Center instance.

- Configure an IAM Identity Center instance to connect to your Amazon Q Business application environment with users and groups added. You can also create and connect an IAM Identity Center instance to Amazon Q Business from the Amazon Q Business console. You can only add

users to an IAM Identity Center instance created from the Amazon Q Business and not groups. To add groups, you need to use the IAM Identity Center console.

> **Important**
>
> If you add a user to a group in IAM Identity Center and have given that group access to your application, it can take up to 24 hours for the change to take effect and for the user to be able to access your Amazon Q Business application.

Understanding types of IAM Identity Center instances

There are two types of IAM Identity Center instances: organization instances and account instances. Amazon Q supports both organization and account level IAM Identity Center instances.

> **Important**
>
> Amazon Q Business supports cross-region IAM Identity Center and Amazon Q Business integrations only for organization instances. Amazon Q Business doesn't support cross-region IAM Identity Center integrations for account level instances. Same-region Amazon Q Business and IAM Identity Center integrations are supported for both organization and account level instances.

The following section provides a brief overview of both instance types. For in-depth distinctions between the two and prerequisites for enabling them, see Manage instances in the IAM Identity Center User Guide.

Topics

- Organization instances
- Account instances

Organization instances

When you enable IAM Identity Center in conjunction with AWS Organizations, you're creating an organization instance of IAM Identity Center. AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and

centrally manage. Your organization instance must be enabled in your management account and you can centrally manage the access of users and groups with a single organization instance. This is the AWS recommended approach to managing workforce identities.

To learn how to create and manage IAM Identity Center organization instances, see the following content in the IAM Identity Center User Guide:

- Enabling an organization instance of IAM Identity Center
- Prerequisites and considerations for setting up IAM Identity Center
- Confirm your identity sources in IAM Identity Center
- Get started with common tasks in IAM Identity Center

Account instances

If you don't have plans to adopt IAM Identity Center for your entire organization, you can use an account instance of IAM Identity Center to manage user and group access to Amazon Q Business application. Account instances are bound to a single AWS account and are used only to manage user and group access for supported applications in the same account and AWS Region. You are limited to one account instance per AWS account. You can create an account instance from either of the following:

- A member account in AWS Organizations.
- A standalone AWS account that is not managed by AWS Organizations.

An account instance may fit your use case if:

- You are trying out Amazon Q Business, and you haven't yet decided that you want to deploy it to your entire organization.
- You are the administrator of a single AWS account within an organization. Instead of waiting for the administrator of your organization to implement Amazon Q Business, you want to go ahead and do it just for the AWS account that you control.
- Your enterprise is large, and does not have a single identity provider, or a single identity store, containing the entire user base that you want to give access to Amazon Q Business.

To learn how to create and manage IAM Identity Center account instances, see the following content in the IAM Identity Center User Guide:

- Account instances of IAM Identity Center
- Enable an account instance of IAM Identity Center
- Control account instance creation with Service Control Policies
- Create an account instance of IAM Identity Center
- Get started with common tasks in IAM Identity Center

Creating a same-region integration

If you don't have an existing IAM Identity Center instance to integrate with Amazon Q Business, we recommend creating one in a region Amazon Q Business is available in.

You can enable and configure an IAM Identity Center instance before you start to create your Amazon Q Business application in the IAM Identity Center console. If you pre-configure an IAM Identity Center instance, you add users and groups in the IAM Identity Center console. Then, during the application creation process, Amazon Q Business automatically detects—and connects to—your already configured IAM Identity Center instance. You add Amazon Q Business subscriptions to your IAM Identity Center users in the Amazon Q Business console.

Or, you can create an IAM Identity Center instance from within the Amazon Q Business console during the Amazon Q Business application creation process. If you choose this option, keep in mind that you can only create and add users to your application using this method. You can add groups you've already created in your IAM Identity Center instance, but can't create them. All groups need to be created from the IAM Identity Center console.

Amazon Q Business supports same-region IAM Identity Center and Amazon Q Business integrations for both organization and account level instances.

Creating a cross-region integration

Amazon Q Business, including Amazon Q Apps, can also integrate with IAM Identity Center in any commercial region where IAM Identity Center is available (excluding opt-in and special regions), even if that region isn't one of the regions supported by Amazon Q Business. You can choose to create a cross-region integration if you already have an IAM Identity Center instance configured in a region that Amazon Q Business isn't currently available in.

When you create a cross-region Amazon Q Business and IAM Identity Center-integration, you enable Amazon Q Business to make cross-region calls in order to access and store information

from your IAM Identity Center instance, such as user and group attributes. This functionality allows Amazon Q Business to support IAM Identity Center-enabled applications in regions different from where your IAM Identity Center instance is ingested. When you create a cross-region integration, your Amazon Q Business application will have access to user and group information from an IAM Identity Center instance deployed in a different region. In these cross-region calls, Amazon Q Business might send the following user attributes:

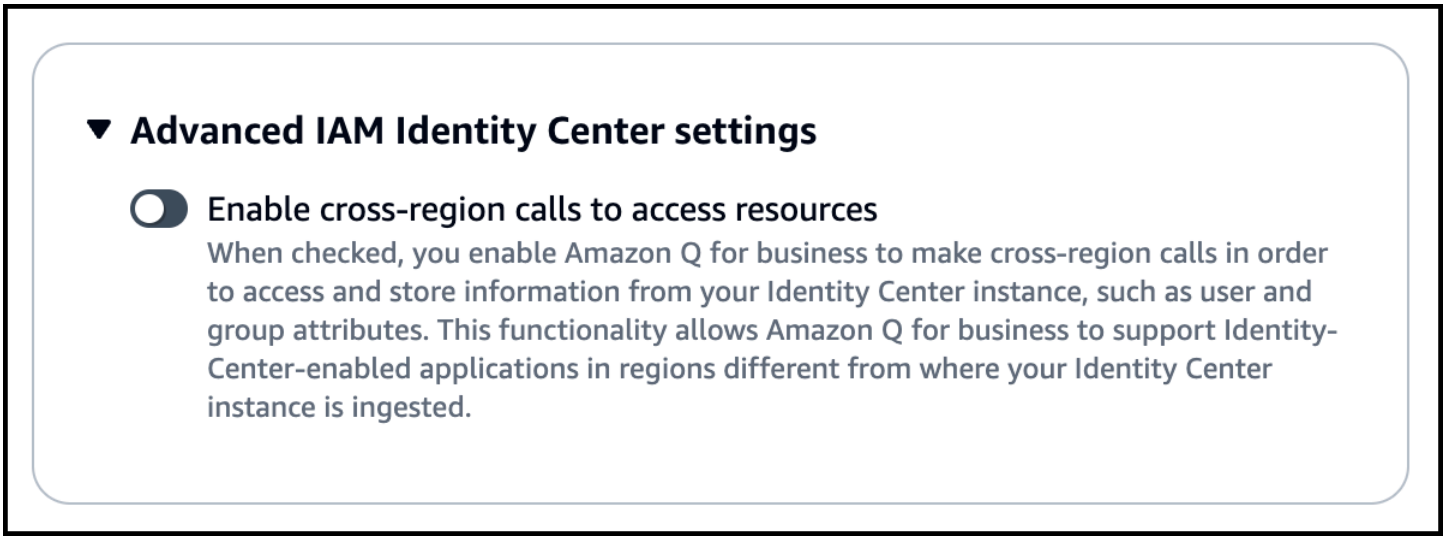
- Email address
- Account in AWS Organizations
- User ID
- Group name
- Group ID

> **Important**
>
> Amazon Q Business supports cross-region IAM Identity Center and Amazon Q Business integrations only for organization level instances. Amazon Q Business doesn't support cross-region IAM Identity Center integrations for account level instances. For more information on IAM Identity Center instance types and their use cases, see Understanding types of IAM Identity Center instances.

If you create a cross-region integration between an Amazon Q Business application and an IAM Identity Center instance, you may experience higher latency when using Amazon Q Business due to the increased overhead of making cross-region calls. The increase in latency will be proportional to the distance of the Amazon Q Business region from the IAM Identity Center region you're using. We recommend performing latency tests for your specific user case. We don't recommend using this feature if you have more than 100 groups per user in your IAM Identity Center instance.

When you create a cross-region IAM Identity Center and Amazon Q Business integration, any Amazon Q Business indices associated with your application are billed in the Amazon Q Business region they're created in. User subscriptions for an Amazon Q Business application using a cross-region IAM Identity Center integration are billed in the region the IAM Identity Center instance is created in. For more information on pricing, see Amazon Q Business Pricing.

Once you opt-in, you will see the option to create a cross-region connection during the Amazon Q Business application creation process, as in the following image:



Creating an Amazon Q Business application environment

To create an Amazon Q Business application environment, you can use either the AWS Management Console or the Amazon Q Business API. When you create an application, response generation from large language model (LLM) knowledge is enabled by default.

As a prerequisite, make sure that you complete the setting up tasks and go through the Configuring an IAM Identity Center instance section. If you're using the AWS CLI or the API, make sure that you've created the required IAM roles.

When you create an application environment, you can also choose to create a Amazon Q Business web experience. If you use the console to create an application environment, the web experience is created automatically, unless you choose otherwise. If you use the CreateApplication API operation to create an application environment, use the CreateWebExperience API operation to create your web experience.

When you create an application, you can also add any existing IAM Identity Center users and groups to your Amazon Q Business application. After you add users or groups to an application environment, you can then assign and choose subscription tiers for each user or group. If you don't have an existing IAM Identity Center instance or user, you can create both of these from the Amazon Q Business console when you create your application. You can't create IAM Identity Center groups from the Amazon Q Business console.

Important

You must add, assign, and subscribe at least one user to your Amazon Q Business application environment for it to work as intended. For more information on user subscriptions for an IAM Identity Center-integrated Amazon Q Business application, see Subscriptions for applications using IAM Identity Center.

Note

As of Oct 31, 2024, once you have created a new Amazon Q Business application environment, the default web experience will allow users to interact directly with the LLM to get answers from its general knowledge or uploaded file content, even if the Admin has not yet connected any enterprise data sources.
For existing application environments, the *Allow direct access to LLM* setting will remain as previously configured. For new application environments, the *Allow direct access to LLM* setting will be enabled by default, though Admins can still disable this if desired.

For a consolidated view of your user subscriptions—including a list of subscribed users, their subscription status, and applications, accounts, or services a user can access through their subscriptions—see the Amazon Q subscriptions page.

The following tabs provide a procedure for creating your Amazon Q Business application environment and adding subscriptions using the AWS Management Console and code examples for using the AWS CLI.

Console

To create an application

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. On the **Create application** page, for **What kind of application do you want to build?**, enter the following information for your Amazon Q Business application:

    a. **Application name** – A name for your Amazon Q Business application environment for easy identification. This name is only visible in the AWS Management Console. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000

alphanumeric characters. Amazon Q Business auto-generates an application name for you, unless you choose to enter a custom name.

b. **Outcome** – Select **Web experience** to create a web experience for your application. Amazon Q Business creates a web experience by default when you create an application. If you don't want to create a web experience, unselect this option.

3. For **Access management method**, choose **IAM Identity Center (recommended)**. Then, complete the following steps:

   a. (Optional) **Advanced IAM Identity Center settings – *optional*** – Activate **Enable cross-region calls** to allow Amazon Q Business to connect to an IAM Identity Center instance that exists in a region not already supported by Amazon Q Business. For more information, see Creating a cross-region IAM Identity Center integration.

   b. Then, you will see the following options based on whether you have an IAM Identity Center instance already configured, or need to create one.

      i. If you don't have an IAM Identity Center instance configured, you see the following:

         A. The region your Amazon Q Business application environment is in.

         B. **Specify tags for IAM Identity Center** – Add tags to keep track of your IAM Identity Center instance.

         C. **Create IAM Identity Center** – Select to create an IAM Identity Center instance. Depending on your setup, you may be prompted to create either an account instance, or an organization instance, or be given the option to choose between creating an account instance and an organization instance. The console will display an ARN for your newly created resource after it's created.

      ii. If you have *both* an IAM Identity Center organization instance and an account instance configured, your instances will be auto-detected, and you see the following options:

         A. **Organization instance of IAM Identity Center** – Select this option to manage access to Amazon Q Business by assigning users and groups from the Identity Center directory for your organization.

         B. **Account instance of IAM Identity Center** – Select this option to manage access to Amazon Q Business by assigning existing users and groups from your Identity Center directory.

C. The region your Amazon Q Business application environment is in.

D. **IAM Identity Center** – The ARN for your IAM Identity Center instance.

iii. If you have an IAM Identity Center account instance configured, your account instance will be auto-detected.

iv. If you have an IAM Identity Center organization instance configured, your organization instance will be auto-detected.

v. If your IAM Identity Center instance is configured in an AWS region Amazon Q Business isn't available in, and you haven't activated cross-region IAM Identity Center calls, you will see a message saying that a connection is unavailable with an option to **Switch region**. Once you allow a cross-region connection between Amazon Q Business and IAM Identity Center using **Advanced IAM Identity Center settings**, your cross-region IAM Identity Center instance will be auto-detected by Amazon Q Business.

> **Note**
>
> Selecting **Switch region** will only give you the option to change your AWS Management Console region. To create a cross-region IAM Identity Center connection, use **Advanced IAM Identity Center settings**.

c. In **Quick start user – *optional***, do the following:

i. In **Select user**, choose from the following options:

A. If you've connected a pre-configured IAM Identity Center instance with users and groups already configured, Amazon Q Business detects the users and groups you have configured in IAM Identity Center. In this case, you can select **Choose a user** and, from the dropdown menu that opens, add users and groups directly from your IAM Identity Center directory.

B. If you've created a IAM Identity Center instance from within the Amazon Q Business console for your Amazon Q Business application, you can add a new user to your application and IAM Identity Center instance. Choose **Add new users and groups** and then complete the following steps:

I. In the **Add new users** dialog box that opens, enter the details of your user. Then select **Next** and **Add**.

> **Note**
>
> You can add multiple users by selecting **Add new user** and entering each user's details before you select **Add**.

Then, select **Assign**. The user is automatically added to an IAM Identity Center directory.

II. The details you must enter for each user include:

- **Username** – A username is required for a user to sign into the AWS access portal. You can't change the username later. Maximum length 128 characters. Can only contain alphanumeric characters or any of the following: +=,.@-_
- **First name** – First name of user.
- **Last name** – Last name of user.
- **Email address** – Email address of user.
- **Confirm email address** – Enter email address again to confirm it.
- **Display name** – The display name assigned to your user.

ii. For **Select subscription** – Choose between **Q Business Pro** and **Q Business Lite**

> **Note**
>
> Amazon Q Business assigns Q Business Pro subscriptions to users and groups by default. To learn more about subscription tiers, see User subscription tiers.

> **Important**
>
> If you add a user to a group in IAM Identity Center and have given that group access to your application, it can take up to 24 hours for the change to take effect and for the user to be able to access your Amazon Q Business application.

4. For **Application details** – Amazon Q Business chooses the following configuration settings for your application by default:

   a. For **Application service access** – Amazon Q Business will create a new service-linked role for your application.

   b. **Encryption** – Amazon Q Business will create an AWS owned AWS KMS key to encrypt your data.

   c. **Web experience service access** – If you've chosen to create a web experience, Amazon Q Business creates a service access role to allow end users to log in to a Amazon Q Business web experience.

5. (Optional) To customize **Application details**, expand the **Application details section**, and then do the following:

   a. In **Application service access**, for **Choose a method to authorize Amazon Q Business**, choose from the following options:

      i. **Create and use a new service-linked role (SLR)** – Create and use a new Amazon Q Business-managed IAM role to allow it to access the AWS resources it needs to create your application.

      ii. **Create and use a new service role (SR)** – Create and use a new IAM role for Amazon Q Business to allow it to access the AWS resources it needs to create your application.

      iii. **Use an existing service role (SR)/service-linked role (SLR)** – Use an existing service role or service-linked IAM role to allow Amazon Q Business to access the AWS resources it needs to create your application.

      > **Note**
      >
      > For more information about example service roles, see IAM role for an Amazon Q Business application. For information on service-linked roles, including to manage them, see Using service-linked roles.

      iv. **Service role name** – A name for the service (IAM) role you created for easy identification on the console.

   b. For **Encryption** – Amazon Q Business encrypts your data by default using AWS managed AWS KMS keys. To customize your encryption settings, select **Customize**

encryption settings (advanced). Then, you can choose to use an existing AWS KMS key or create a new one.

c. In **Web experience service access**, enter the following information:

i. For **Choose a method to authorize Amazon Q Business** – A service access role assumed by end users when they sign in to your web experience that grants them permission to start and manage conversations Amazon Q Business. You can choose to use an existing role or create a new role.

ii. **Service role name** – A name for the service role you created for easy identification on the console.

6. To start creating your application, choose **Create**.

> **Note**
>
> If you're creating a web experience, you can also choose to create your application and view and customize your web experience by selecting **Create and open web experience**.

AWS CLI

To configure an Amazon Q Business application

```
aws qbusiness create-application \
--display-name application-name \
--identity-center-instance-arn identity-center-instance-arn \
--role-arn roleArn \
--description application-description \
--encryption-configuration kmsKeyId=<kms-key-id> \
--attachments-configuration attachmentsControlMode=ENABLED
```

To add users to an application environment

```
aws sso-admin create-application-assignment \
--application-arn idc-app-arn \
--principal-id idc-user-ID \
--principal-type USER
```

To provision a user subscription

```
aws qbusiness create-subscription \
--application-id application-id \
--principal user=idc-user-id \
--type subscription-type
```

To add groups to an application environment

```
aws sso-admin create-application-assignment \
--application-arn idc-app-arn \
--principal-id idc-group-ID \
--principal-type GROUP
```

To provision a group subscription

```
aws qbusiness create-subscription \
--application-id application-id \
--principal group=idc-group-id \
--type subscription-type
```

Migrating an Amazon Q Business direct SAML 2.0 application to IAM Identity Center

Important

This content applies only to Amazon Q Business applications that need to migrate from using legacy SAML identity management to using IAM Identity Center for user access management.

To migrate an Amazon Q Business application connected directly to an external identity provider (IdP) to IAM Identity Center for user access management, follow the steps in this section.

If your existing external IdP application is connected to a supported Amazon Q Business data source connector that already has access control (ACL) and identity crawling enabled, it's ready to migrate to IAM Identity Center. If your existing external IdP application is connected to a supported Amazon Q Business data source connector that doesn't already have ACL or identity crawling enabled, you need to first enable these before you can begin migrating your application to IAM Identity Center. You do this by updating your application.

If you've not used IAM Identity Center before, Amazon Q Business will give you the option to create an IAM Identity Center instance from the Amazon Q Business console as part of the migration path. However, we recommend configuring an IAM Identity Center instance before migrating your existing SAML 2.0 compliant application to IAM Identity Center, especially if you're planning to connect your IAM Identity Center to an Active Directory or external identity provider. If you're managing users and groups in one identity source, changing to a different identity source might remove all user and group assignments.

For important information on creating an IAM Identity Center instance for your Amazon Q Business application, see Configuring an IAM Identity Center instance.

The following tabs provide a procedure for migrating an existing, legacy SAML 2.0 based Amazon Q Business application to IAM Identity Center using the AWS Management Console and the AWS CLI.

Topics

- Migrating an application

Migrating an application

The following tabs provide a procedure for migrating your application on the AWS Management Console and code examples for the AWS CLI.

Console

To migrate an Amazon Q Business application

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your SAML 2.0 integrated application from the list of applications.
3. In **Advanced IAM Identity Center settings**, activate **Enable cross-region calls** to access resources to allow Amazon Q Business to connect to an IAM Identity Center instance that

exists in a region not already supported by Amazon Q Business. For more information, see Creating a cross-region IAM Identity Center integration.

4. Then, depending on your Amazon Q Business application configuration you will see one of the following:

   a. If the **Connect to IAM Identity Center** banner on the top of the page asks you to activate your ACL and identity crawling in preparation for migrating your application, you will need to activate ACL and identity crawling for the data sources connected to your application before migrating your application to IAM Identity Center. To do this, update your application. Then, move to the next step.

   b. If the **Connect to IAM Identity Center** banner on the top of the page displays a **Connect to IAM Identity Center** option, it means ACL and identity crawling are already enabled for your application and it's ready to migrate to IAM Identity Center. You can move to the next step.

5. From the **Connect to IAM Identity Center** banner on the top of the page, select **Connect to IAM Identity Center**.

6. In **Connect Amazon Q Business to IAM Identity Center**, you will see the following options based on whether you have an IAM Identity Center instance already configured, or need to create one.

   1. If you don't have an IAM Identity Center instance configured, you see the following:

      - The region your Amazon Q Business application is in. This is so you can make sure that the region for your Amazon Q Business application and IAM Identity Center instance match.
      - **Specify tags for IAM Identity Center** – Add tags to keep track of your IAM Identity Center instance.
      - **Create IAM Identity Center** – Select to create a minimally-configured IAM Identity Center instance. The console will display an ARN for your newly created resource after it's created.

   2. If you have *both* an IAM Identity Center organization instance and an account instance configured, your instances will be auto-detected, and you see the following options:

      - **Connect to organization instance of IAM Identity Center** – Select this option to manage access to Amazon Q Business by assigning users and groups from the Identity Center directory for your organization.

- **Connect to account instance of IAM Identity Center** – Select this option to manage access to Amazon Q Business by assigning existing users and groups from your Identity Center directory.
- The region your Amazon Q Business application is in. This is so you can make sure that the region for your Amazon Q Business application and IAM Identity Center instance match.
- **IAM Identity Center** – The ARN for your IAM Identity Center instance.

3. If you have an IAM Identity Center account instance configured, your account instance will be auto-detected and you will see the following:
   - The region your Amazon Q Business application is in. This is so you can make sure that the region for your Amazon Q Business application and IAM Identity Center instance match.
   - **IAM Identity Center** – The ARN for your IAM Identity Center instance.
4. If you have an IAM Identity Center organization instance configured, you will see a message asking you to tell your admin to give you access to IAM Identity Center. You will need access to IAM Identity Center before you can proceed.

> **Note**
>
> If you plan to connect your IAM Identity Center to an Active Directory or external identity provider we recommend canceling this setup and configuring IAM Identity Center from the IAM Identity Center console. If you're managing users and groups in one identity source, changing to a different identity source might remove all user and group assignments.

7. From the application summary page, select **Groups and users**, and add users.

> **Note**
>
> If you plan to add groups to your application create these groups in IAM Identity Center before you create your application. If you don't have already configured IAM Identity Center groups, Amazon Q Business will redirect you to the IAM Identity Center console to configure groups before you can add them to your applicaton.

8. Then, from the application summary page, select **Migrate application** from the banner on the top of the page.
9. In the **Migrate application traffic** dialog box that opens, for **Service access**, choose an existing service role or create a new one. Amazon Q Business needs these permissions to access the resources it needs to migrate your application. For more information on the permissions required, see IAM role for Amazon Q Business data source connectors.
10. Select **Migrate**.

    When the migration is complete, the console displays a **Successfully migrated application traffic to IAM Identity Center** message.

AWS CLI

To migrate an Amazon Q Business application

Before starting the migration process, confirm the presence of you web experience using the following command:

```
aws qbusiness list-web-experiences \
--application-id application-id
```

If the `list-web-experiences` command returns a `webExperienceId`, you can proceed with migrating your application regardless of the status of the web experience.

If the `list-web-experiences` command doesn't return a `webExperienceId`, you *must* create a new web experience before proceeding with migration using the following command:

```
aws qbusiness create-web-experience \
--application-id application-id
```

Then, update your Amazon Q Business application using the following command:

```
aws qbusiness update-application \
--application-id application-id \
--identity-center-instance-arn idc-instance-arn
```

Wait for your application status to change from `UPDATING` to `ACTIVE`. The response should include the `identityCenterApplicationArn` as one of the response fields. Check this is the case using the following command:

```
aws qbusiness get-application \
--application-id application-id
```

After your application status changes to `UPDATING`, add users and groups to your application using the following commands:

To add users to an application

```
aws sso-admin create-application-assignment \
--application-arn idc-app-arn \
--principal-id idc-user-ID \
--principal-type USER
```

To add groups to an application

```
aws sso-admin create-application-assignment \
--application-arn idc-app-arn \
--principal-id idc-group-ID \
--principal-type GROUP
```

Then, update your Amazon Q Business web experience using the following command:

```
aws qbusiness update-web-experience \
--role-arn role-arn-value \
--application-id application-id \
--web-experience-id web-experience-id
```

> **Note**
>
> For IAM role permissions required, see IAM role for an Amazon Q Business web experience.

Making authenticated Amazon Q Business API calls using IAM Identity Center

Important

This documentation is for developers building custom applications that integrate with Amazon Q Business APIs. These instructions help you create a trusted backend component in your custom application that can make authenticated API calls on behalf of your users. This is NOT for the built-in Amazon Q Business web experience — that handles authentication automatically through the AWS console.

Amazon Q Business can securely handle data with integrated authentication and authorization. During data ingestion, Amazon Q Business preserves the authorization information—access control lists (ACLs)—from the data source so users can only request answers from the data they already have access to. Through IAM Identity Center, Amazon Q Business uses trusted identity propagation to ensure that an end user is authenticated and receives fine-grained authorization to their user ID and group-based resources.

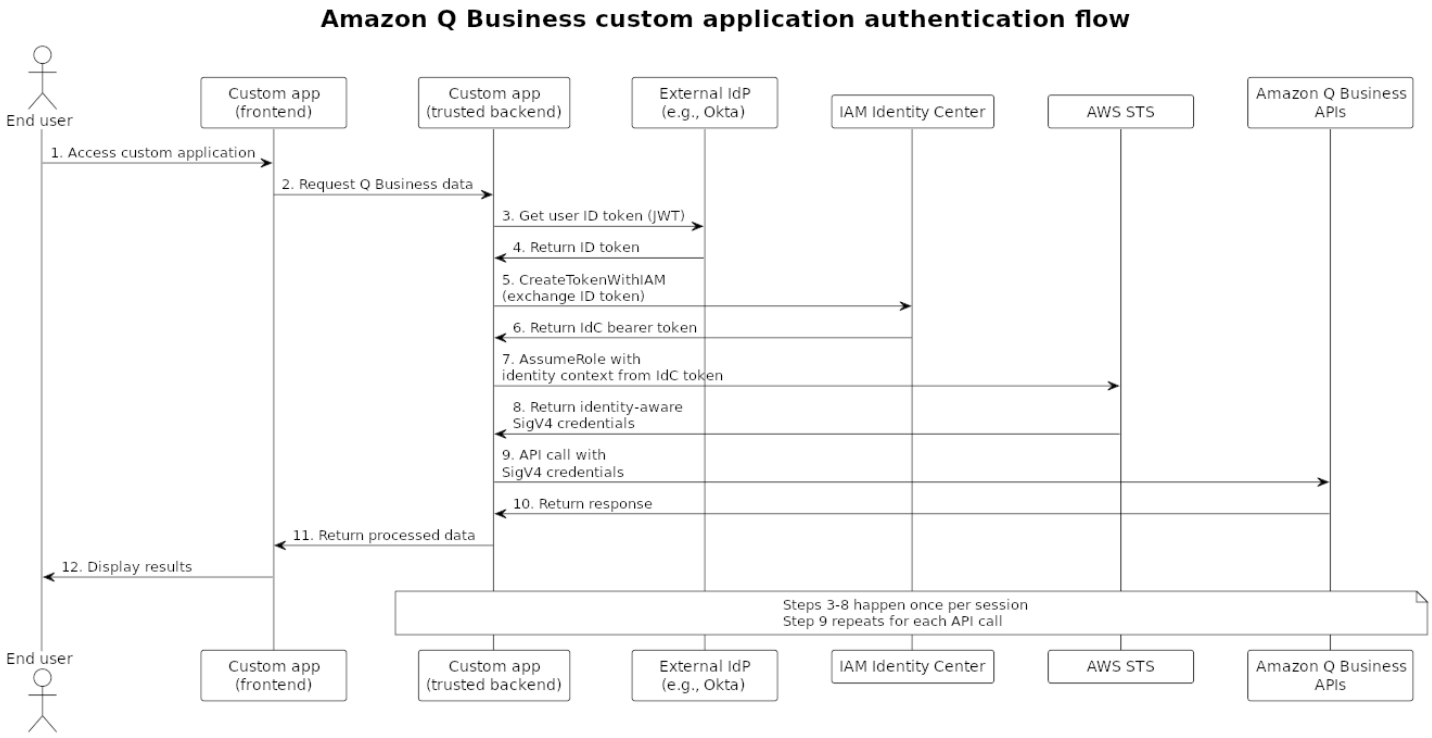
In order to achieve this, a subset of the Amazon Q Business APIs (Chat, ChatSync, SearchRelevantContent, ListConversations, ListMessages, DeleteConversation, PutFeedback) require identity-aware AWS Sig V4 credentials for the authenticated user on whose behalf the API call is being made.

Note

This page provides an overview of the workflows needed to obtain AWS Sig V4 credentials for a user authenticated using an OIDC-compliant external identity provider (IdP), such as Okta. While we use Okta as an example, the same principles and steps apply to any other identity provider synced with your IAM Identity Center instance.

Architecture overview

The following diagram shows how your custom application components interact with AWS services to make authenticated API calls:



Key components:

- **Custom app frontend**: Your user-facing application (web, mobile, etc.)
- **Custom app trusted backend**: Your server-side component that handles AWS API calls
- **External IdP**: Your identity provider (Okta, Azure AD, etc.)
- **IAM Identity Center**: AWS service that manages identity federation
- **Amazon Q Business APIs**: The APIs your application calls (`Chat`, `SearchRelevantContent`, etc.)

> **Note**
>
> Your custom application's backend component must implement this authentication flow. End users interact with your frontend, which communicates with your trusted backend to make Amazon Q Business API calls.

Topics

- Prerequisites
- One-time setup

- Workflow for custom application backend API calls for an authenticated user

Prerequisites

Before you begin setting up for making Sig V4 authenticated API calls, make sure you've done the following:

- Created an Amazon Q Business application.
- Created an Okta IdP instance and configured users and groups within it. While we use Okta as an example, the same principles and steps apply to any other OIDC-compliant external identity provider synced with your IAM Identity Center instance.
- Created an IAM Identity Center instance for your Amazon Q Business application that uses Okta as your as the identity source.
- Synchronized the users and groups from Okta with IAM Identity Center.
- Configured access to the AWS CLI.

One-time setup

The following section outlines the steps to set up the Amazon Q Business control plane. You only need to perform these steps once.

1. Create an OIDC app integration in Okta.
2. Then, in the IAM Identity Center instance you have created, create a Trusted Token Issuer to trust IdP issuer with the issuer URL. For example, *https://<your-okta-instance>.okta.com/oauth2/default*.
3. In your IAM Identity Center instance, create a customer managed custom application using the following AWS CLI command:

```
aws sso-admin create-application \
--application-provider-arn arn:aws:sso::aws:applicationProvider/custom \
--instance-arn your-identity-center-arn \
--name your-custom-application-name
```

4. Then, disable user assignment or provide explicit user assignments to the custom application you created using the following AWS CLI command:

```
aws sso-admin put-application-assignment-configuration \
--application-arn your-custom-application-arn \
--no-assignment-required
```

5. Then, add a JWT bearer grant to your application environment using the put application environment grant CLI command. For example:

```
aws sso-admin put-application-grant \
--cli-input-json '{
   "ApplicationArn":"identity-center-custom-application-arn",
   "Grant":{
      "JwtBearer":{
         "AuthorizedTokenIssuers":[
            {
               "AuthorizedAudiences":[
                  "idp-authorized-audience"
               ],
               "TrustedTokenIssuerArn":"trusted-token-issuer-arn"
            }
         ]
      }
   },
   "GrantType":"urn:ietf:params:oauth:grant-type:jwt-bearer"
}'
```

6. You will then need to add an authentication method for a Amazon Q Business application environment using the put application environment authentication method AWS CLI command:

```
aws sso-admin put-application-authentication-method \
--cli-input-json '{
    "ApplicationArn": "identity-center-custom-application-arn",
    "AuthenticationMethod": {
        "Iam": {
            "ActorPolicy": {
                "Version": "2012-10-17",
                "Statement": [{
```

```
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "your-aws-account-id",
                        "Service": "qbusiness.amazonaws.com"
                    },
                    "Action": [
                        "sso-oauth:CreateTokenWithIAM"
                    ],
                    "Resource": "your-identity-center-custom-application-arn",
                    "Condition": {
                        "ArnEquals": {
                            "aws:SourceArn": "arn:${ArnPartition}:${Service}:
${Region}:${AppAccountId}:${Resource}"
                        },
                        "StringEquals": {
                            "aws:SourceAccount": "${AppAccountId}"
                        }
                    }
                }]
            }
        }
    },
    "AuthenticationMethodType": "IAM"
}'
```

7. Next, add a list of authorized targets for an IAM Identity Center access scope for an Amazon Q Business application environment using the following put application environment access scope AWS CLI command:

```
aws sso-admin put-application-access-scope \
--application-arn identity-center-custom-application-arn \
--scope "qbusiness:conversations:access"
```

8. Then, create an IAM role that your application environment will use to call AssumeRole API with the following policies:

   Trust policy

   JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [{
        "Sid": "QCLITrustPolicy",
        "Effect": "Allow",
        "Principal": {
            "Service": [
                "qbusiness.amazonaws.com"
            ]
        },
        "Action": [
            "sts:AssumeRole",
            "sts:SetContext"
        ],
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "111122223333"
            }
        }
    }]
}
```

Permissions policy

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessConversationPermission",
            "Effect": "Allow",
            "Action": [
                "qbusiness:Chat",
                "qbusiness:ChatSync",
                "qbusiness:ListMessages",
                "qbusiness:ListConversations",
                "qbusiness:DeleteConversation",
                "qbusiness:PutFeedback",
                "qbusiness:GetWebExperience",
                "qbusiness:GetApplication",
                "qbusiness:ListPlugins",
                "qbusiness:GetChatControlsConfiguration",
```

```
                "qbusiness:GetMedia"
            ],
            "Resource": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
        },
        {
            "Sid": "QBusinessKMSDecryptPermissions",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/key-id"
            ]
        },
        {
            "Sid": "QBusinessSetContextPermissions",
            "Effect": "Allow",
            "Action": "sts:SetContext",
            "Resource": "arn:aws:sts:*:111122223333:assumed-role/role-
name/session-name"
        }
    ]
}
```

9. Then, get the list of synced users and groups in your IAM Identity Center-integrated Amazon Q Business application using the following AWS CLI command:

```
aws sso-admin list-application-assignments \
--application-arn your-custom-application-arn
```

10. Finally, add a subscription for each user or group in your IAM Identity Center-integrated Amazon Q Business application using the following AWS CLI commands:

To provision a user subscription

```
aws qbusiness create-subscription \
--application-id application-id \
--principal user=idc-user-id \
--type subscription-type
```

To provision a group subscription

```
aws qbusiness create-subscription \
--application-id application-id \
--principal group=idc-group-id \
--type subscription-type
```

Workflow for custom application backend API calls for an authenticated user

After you've completed the one-time setup tasks, you can use one of two workflows to generate identity-aware credentials to make API calls for your IAM Identity Center-integrated Amazon Q Business application:

- the AWS SDK trusted identity propagation plugin (TIP_ workflow (recommended), or a longer API workflow.
- The API workflow requires a manual token exchange with IAM Identity Center and uses AWS STS to generate identity-aware credentials for your Amazon Q Business application.

The AWS SDK TIP plugin workflow streamlines the authorization process by eliminating the need for manual token exchange and credential generation. Once set up, it automatically handles token exchange and credential management.

The TIP plugin workflow is the recommended approach for implementing identity-aware authorization. It is currently supported by the Java and JavaScript SDK. For more information, see Trusted identity propagation (TIP) plugin in the *AWS SDKs and Tools Reference Guide*.

(Recommended) Using an SDK plugin workflow

Use the Java or JavaScript SDK to create the plugin and make calls to Amazon Q Business using the following:

- `webTokenProvider` – A function that the customer implements to obtain an OpenID token from their external identity provider.

- `accessRoleArn` – The IAM role ARN to be assumed by the plugin with the user's identity context to get the identity-enhanced credentials.
- `applicationArn` – The unique identifier string for the client or application. This value is an application ARN that has OAuth grants configured.
- `applicationRoleArn` – The IAM role ARN to be assumed with `AssumeRoleWithWebIdentity` so that the OIDC and AWS STS clients can be bootstrapped. If `applicationRoleArn` is not provided, it is mandatory to provide both `ssoOidcClient` and `stsClient` parameters.
- `ssoOidcClient` – An IAM Identity Center OIDC client, such as `SsoOidcClient` for Java or `client-sso-oidc` for Javascript, with customer-defined configurations. If not provided, an OIDC client using `applicationRoleArn` will be instantiated and used.
- `stsClient` – An AWS STS client with customer-defined configurations, used to assume `accessRoleArn` with the user's identity context. If not provided, an AWS STS client using `applicationRoleArn` will be instantiated and used.

If both `ssoOidcClient` and `stsClient`, and `applicationRoleArn` are provided, the former is prioritized.

```
// Option-1: Build and pass OIDC and STS clients
SsoOidcClient oidcClient = SsoOidcClient.builder()
    .region(Region.US_EAST_1)
    .credentialsProvider(credentialsProvider).build();

StsClient stsClient = StsClient.builder()
    .region(Region.US_EAST_1)
    .credentialsProvider(credentialsProvider).build();

TrustedIdentityPropagationPlugin trustedIdentityPropagationPlugin =
 TrustedIdentityPropagationPlugin.builder()
        .webTokenProvider(() -> webToken)
        .applicationArn(idcApplicationArn)
        .accessRoleArn(accessRoleArn)
        .ssoOidcClient(client)
        .stsClient(stsClient)
        .build();

// Option-2: Pass applicationRoleArn and defer the STS & OIDC clients creation to the
 plugin
```

```
TrustedIdentityPropagationPlugin trustedIdentityPropagationPlugin =
 TrustedIdentityPropagationPlugin.builder()
        .webTokenProvider(() -> webToken)
        .applicationArn(idcApplicationArn)
        .accessRoleArn(accessRoleArn)
        .applicationRoleArn(applicationRoleArn)
        .build();

QBusinessClient qBusinessClient = QBusinessClient.builder()
        .region(Region.US_EAST_1)
        .addPlugin(trustedIdentityPropagationPlugin)
        .build();

// Create ChatSyncRequest
ChatSyncRequest chatSyncRequest = ChatSyncRequest.builder()
        .applicationId(applicationId)
        .userMessage(userMessage)
        // You can add conversationId, attachments, chatMode, etc. here
        .build();

// Call chatSync operation
ChatSyncResponse chatSyncResponse = qBusinessClient.chatSync(chatSyncRequest);
```

Using an API workflow

1. First, use the CreateTokenWithIAM API call to obtain an IAM Identity Center-provided JWT bearer grant token using your:
   - **`clientID`**: Your IAM Identity Center custom application environment ARN.
   - **`grantType`**: For example, *`'urn:ietf:params:oauth:grant-type:jwt-bearer'`*.
   - **`assertion`**: The user authenticated ID token obtained from Okta.
2. Then, use the AssumeRole API call to obtain user decorated AWS Sig V4 credentials using your:
   - **`RoleArn`**: The IAM role ARN.
   - **`RoleSessionName`**: A unique session name.
   - **`DurationSeconds`**: The session duration in seconds.
   - **`ProvidedContexts`**: A list of previously acquired trusted context assertions in the format of a JSON array. The trusted context assertion is signed and encrypted by AWS STS. For example:

```
[{
    'ProviderArn': "arn:aws:iam::aws:contextProvider/IdentityCenter",
    'ContextAssertion': claims["sts:identity_context"]
}]
```

> **Note**
>
> The `ContextAssertion` uses the “sts:identity_context” object from the claims object of the decoded JWT bearer grant token obtained as part of Step 1 in this procedure.

3. Use the identity-aware AWS Sig V4 credentials in the previous step to initialize the AWS SDK client and then make Amazon Q Business API calls using that client.

   First, set the following environment variables in your command line environment:

   ```
   AWS_ACCESS_KEY_ID="identity-aware-sigv4-access-key"
   AWS_SECRET_ACCESS_KEY="identity-aware-sigv4-secret-key"
   AWS_SESSION_TOKEN="identity-aware-sigv4-session-token"
   ```

   Then, run the following Python script from the same window:

   ```
   import boto3
   import json
   import random

   import boto3

   aq_client = boto3.client(
       "qbusiness",
       region_name="your-aws-region"
   )

   resp = aq_client.chat_sync(
       applicationId = "amazon-qbusiness-application-id",
       userMessage = "chat-request",
       clientToken = str(random.randint(0,10000)
   )
   ```

```
print(f"Amazon Q Business response: {resp["systemMessage"]}")
```

> **Important**
>
> As a security best practice, the credentials should not be hard coded in your scripts or code. For more information, refer to Boto 3 documentation on using credentials.

Managing Amazon Q Business application resources

You can choose to manage your Amazon Q Business application environment and associated resources. To learn how to do so, see the following sections:

- Managing Amazon Q Business applications
- Managing Amazon Q Business web experiences
- Managing user subscriptions
- Tagging resources

Managing Amazon Q Business applications

To manage an Amazon Q Business application environment, you can take the following actions:

Actions

- Deleting an application
- Getting application environment properties
- Listing applications
- Updating an application environment

Deleting an application

To delete an Amazon Q Business application environment, you can use the console or the DeleteApplication API operation.

The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To delete an Amazon Q Business application

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, choose **Actions**.
3. Choose **Delete**.
4. In the dialog box that opens, type **`Delete`** to confirm deletion, and then choose **Delete**.

   You are returned to the service console while your application environment is deleted. When the deletion process is complete, the console displays a message confirming successful deletion.

AWS CLI

To delete an Amazon Q Business application environment

```
aws qbusiness delete-application \
--application-id application-id
```

Getting application environment properties

To get the properties of an Amazon Q Business application environment, you can use the console or the GetApplication API operation.

The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To get properties of an Amazon Q Business application environment

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. For **Applications**, select the name of your application environment from the list of applications.
3. On **Application settings**, the following properties are available:

   - **Application name** – The name that you chose for your application environment.

- **Application ID** – The ID assigned to your application environment.
- **Subtitle** – The subtitle that you chose to assign to your application environment.
- **Service access** – The service access role that your application environment is using.
- **Title** – The title that you gave to your application environment.
- **Application status** – The status of your application environment.

To update a setting, select **Edit**.

AWS CLI

To get Amazon Q Business application properties

```
aws qbusiness get-application \
--application-id application-id
```

Listing applications

To list Amazon Q Business applications, you can use the console or the ListApplications API operation.

The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To list your Amazon Q Business application environments

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, all your configured application environments are listed.

AWS CLI

To list Amazon Q Business application environments

```
aws qbusiness list-applications \
```

```
--max-results max-results-to-return
```

Updating an application environment

To update an Amazon Q Business application environment, you can use the console or the UpdateApplication API operation.

> **Note**
>
> You can't update the retriever you've chosen or change users and groups added to the application environment when you update it. If you need to update your retriever, create a new application environment.
> If you're integrating your Amazon Q Business application environment with IAM Identity Center (IDC) and you want to update users and groups, you can do so from the application environment summary page.

The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To update an Amazon Q Business application environment

Option 1

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. In **Applications**, choose **Actions**.
4. Choose **Edit**.

   On the **Update application** page, edit your application environment settings.

Option 2

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.

3. On the application page, select **Edit** from the page header, or select **Edit** from **Application settings**.
4. Choose **Edit**.

   On the **Update application** page, edit your application environment settings.

AWS CLI

To update an Amazon Q Business application environment

```
aws qbusiness update-application \
--application-id application-id \
--display-name application-name \
--role-arn roleArn \
--description application-description \
--attachments-configuration attachmentsControlMode=ENABLED
```

Managing Amazon Q Business web experiences

To manage Amazon Q Business web experiences, you can take the following actions:

Actions

- Creating a web experience
- Deleting a web experience
- Getting properties of a web experience
- Listing web experiences
- Updating a web experience

Creating a web experience

To create an Amazon Q Business web experience, you can use the console or the CreateWebExperience API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

If you use the console, this action is spread across two steps: Configuring an Amazon Q Business application using AWS IAM Identity Center and Customizing web experience. To create a web experience, you must create an application environment.

AWS CLI

To create an Amazon Q Business web experience

```
aws qbusiness create-web-experience \
--application-id application-id \
--sample-prompts-control-mode sample-prompts \
--subtitle subtitle \
--tags tags \
--title title \
--welcome-message welcome-message \
```

Deleting a web experience

To delete an Amazon Q Business web experience, you can use the console or the DeleteWebExperience API operation.

If you're using the API, you can delete a web experience without deleting the application environment that it's a part of.

If you're using the console, the only way to delete your Amazon Q Business web experience is to delete the Amazon Q Business application environment that it's attached to.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To delete an Amazon Q Business web experience

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, choose **Actions**.
3. Choose **Delete**.

4. In the dialog box that opens, type **`Delete`** to confirm deletion, and then choose **Delete**.

   You are returned to the service console while your application environment is deleted. When the deletion process is complete, the console displays a message confirming successful deletion. Both the application environment and the web experience are deleted.

AWS CLI

To delete an Amazon Q Business web experience

```
aws qbusiness delete-web-experience \
--application-id application-id \
--web-experience-id web-experience-id
```

Getting properties of a web experience

To get the properties of an Amazon Q Business web experience, you can use the console or the GetWebExperience API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To get properties of an Amazon Q Business web experience

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. For **Web experience settings**, the following settings are available:

   - **Web experience IAM role ARN** – The IAM role assumed by end users when they log in to your web experience.
   - **Deployed URL** – The deployed URL of your web experience.
   - **Tags** – Tags that are attached to your web experience.

   To update a setting, choose **Edit**.

AWS CLI

To get properties of an Amazon Q Business web experience

```
aws qbusiness get-web-experience \
--application-id application-id \
--web-experience-id web-experience-id
```

Listing web experiences

To list Amazon Q Business web experiences, you can use the console or the ListWebExperiences API operation.

If you use the console, you can only see the web experience that's attached to a single application environment.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To list Amazon Q Business web experiences

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. For **Applications**, the Amazon Q Business web experience attached to your application environment is shown.

AWS CLI

To list Amazon Q Business web experiences

```
aws qbusiness get-web-experience \
--application-id application-id \
--web-experience-id web-experience-id \
--max-results max-results-to-return
```

Updating a web experience

To update an Amazon Q Business web experience, you can use the console or the UpdateWebExperience API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To update an Amazon Q Business web experience

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. Select **Customize web experience**.
4. Expand the right navigation menu to edit your web experience settings.

AWS CLI

To update an Amazon Q Business web experience

```
aws qbusiness update-web-experience \
--application-id application-id \
--web-experience-id web-experience-id \
--authentication-configuration authentication-configuration \
--sample-prompts-control-mode sample-prompts \
--subtitle subtitle \
--title title \
--welcome-message welcome-message
```

Managing user subscriptions for IAM Identity Center-integrated applications

To manage user subscriptions added to an application environment, you can perform the following actions:

Actions

- Updating user subscriptions
- Canceling user or group subscriptions
- Listing user subscriptions

Updating user subscriptions

To update a subscription in an Amazon Q Business application, you can use either the AWS Management Console or the UpdateSubscription API operation.

For more information on user subscriptions for an IAM Identity Center-integrated Amazon Q Business application, see Subscriptions for applications using IAM Identity Center.

Console

To update user or group subscription tier

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of the application environment you created.
3. From your applications page, from the **User access** section, select **Manage user access**.
4. From **Manage access and subscriptions** select the subscription you want to update. Then, select **Edit subscription**.
5. In the **Confirm subscription change** dialog box that opens, from the **New subscription** dropdown select **Q Business Lite** or **Q Business Pro**.
6. Then, select **Confirm**. You will see the subscription status notification change next to the user you've added the subscription to.
7. Then, select **Confirm** to save your changes.

AWS CLI

To update user or group subscription tier

```
aws qbusiness update-subscription \
--application-id application-id \
--subscription-id subscription-id \
--type subscription-type
```

Canceling user or group subscriptions

To cancel subscriptions, you can use the AWS Management Console or the CancelSubscription API operation.

When you unsubscribe and remove a user or group, it unsubscribes them from the application environment and removes them from the user list.

For more information on user subscriptions for an IAM Identity Center-integrated Amazon Q Business application, see Subscriptions for applications using IAM Identity Center.

Console

To unsubscribe a user or group from an Amazon Q Business application environment

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of the application environment you created.
3. From your applications page, from the **User access** section, select **Manage user access**.
4. From **Manage access and subscriptions** select the user or group subscription you want to update. Then, select **Remove and unsubscribe**.
5. Then, from the **Unsubscribe and remove** dialog box, **Confirm**.
6. Then, select **Confirm** to save your changes.

   This step cancels subscriptions for the selected users and groups and also removes them from your Amazon Q Business application environment.

> **Note**
>
> To stop subscription charges for a user, ensure you have unsubscribed that user from all Amazon Q Business application environments and Quick instances. For instructions on how to unsubscribe a user from Quick, see Unsubscribing from Quick Q in the Quick User Guide.
> To stop charges for an Amazon Q Business index, you must delete either your Amazon Q Business index or delete your Amazon Q Business application environment. If you use the console, deleting your application environment is the only way to delete an index associated with it.

AWS CLI

To cancel user or group subscriptions to Amazon Q Business

```
aws qbusiness cancel-subscription \
--application-id application-id \
--subscription-id subscription-id \
--type subscription-type
```

Listing user subscriptions

To see a list of user and group subscriptions within a specific Amazon Q Business application, you can use the AWS Management Console or the ListSubscriptions API operation.

For a consolidated view of your user subscriptions—including a list of subscribed users, their subscription status, and applications, accounts, or services a user can access through their subscriptions—you can also view the Amazon Q subscriptions page.

Console

To view a list of user and group subscriptions in an Amazon Q Business application environment

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of the application environment you created.
3. From your applications page, from the **User access** section, select **Manage user access**.
4. In the **Manage access and subscriptions** select **Users** if you want to view user subscriptions or **Groups** if you want to list group subscriptions.

To view a consolidated list of all user and group subscriptions across all Amazon Q Business application environments

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the left navigation menu, choose **Subscriptions**,and then select **Users** if you want to view user subscriptions or **Groups** if you want to list group subscriptions.

AWS CLI

To list user or group subscriptions in an Amazon Q Business application

```
aws qbusiness list-subscriptions \
--application-id application-id
```

To list user or group subscriptions across all Amazon Q Business applications

This action is not supported.

Tagging Amazon Q Business resources

Manage your Amazon Q Business applications and web experiences by assigning tags. You can use tags to categorize your Amazon Q Business resources in various ways. For example, you could categorize by purpose, owner, or application, or any combination. Each tag consists of a *key* and a *value*, both of which you define.

Tags help you to do the following:

- **Identify and organize your AWS resources** – Many AWS services support tagging, so you can assign the same tag to resources in different services to indicate that the resources are related. For example, you can tag an Amazon Kendra retriever and the Amazon Q Business web experience that uses the retriever with the same tag.
- **Allocate costs** – You activate tags on the AWS Billing and Cost Management dashboard. AWS uses tags to categorize your costs and deliver a monthly cost allocation report to you. For more information, see Cost Allocation and Tagging in the *AWS Billing User Guide*.
- **Control access to your resources** – You can use tags in AWS Identity and Access Management (IAM) policies that control access to Amazon Q Business resources. To activate tag-based access control, you can attach these policies to an IAM role or IAM user. For more information, see Authorization based on tags.

You can create and manage tags using the AWS Management Console, the AWS Command Line Interface (AWS CLI), or the Amazon Q Business API.

Topics

- Using tags

- Tag restrictions

Using tags

If you're using the console, you can tag resources when you create them or add them later. You can also use the console to update or remove tags in the following ways:

Adding tags

To add Amazon Q Business tags

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From **Applications**, select the application whose resources you want to tag.
3. From the application summary page, scroll down and select **Tags**.
4. In **Tags**, from the resource you want to add tags to, select **Manage tags**.
5. In **Tags – *optional***, select **Add new tag** to add tags to your Amazon Q Business resource. Then, enter the following information for each tag:
   - **Key** – Add a key for your tag.
   - **Value - *optional*** – An optional value for your tag.
6. Select **Save**.

Removing tags

To remove tags

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From **Applications**, select the application you want to delete tags from.
3. From the application summary page, scroll down and select **Tags**.
4. In **Tags**, from the resource you want to add tags to, select **Manage tags**.
5. In **Tags – *optional***, select **Remove**.
6. Select **Save**.

Listing tags

To view a list of tags

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From **Applications**, select the application you want to delete tags from.
3. From the application summary page, scroll down and select **Tags**.
4. In **Tags**, each tagged resource will display a list of tags associated with it.

If you're using the AWS CLI or the Amazon Q Business API, use the following operations to manage tags for your resources:

- CreateApplication – Apply tags when you create an Amazon Q Business application.
- CreateWebExperience – Apply tags when you create an Amazon Q Business web experience.
- ListTagsForResource – View the tags associated with a resource.
- TagResource – Add and modify tags for a resource.
- UntagResource – Remove tags from a resource.

Tag restrictions

The following restrictions apply to tags on Amazon Q Business resources:

- Maximum number of tags – 50
- Maximum key length – 128 characters
- Maximum value length – 256 characters
- Valid characters for key and value – a–z, A–Z, space, and the following characters: _ . : / = + - and @
- Keys and values are case sensitive
- Don't use `aws:` as a prefix for keys; it's reserved for AWS use

Creating an Amazon Q Business application using Identity Federation through IAM

This section walks you through creating and configuring an Amazon Q Business application using IAM federation to manage end user access.

Amazon Q Business supports identity federation through AWS Identity and Access Management. When you use identity federation, you can manage users with your enterprise identity provider (IdP) and use AWS Identity and Access Management to authenticate users when they sign in to Amazon Q Business.

You can use any third-party identity provider that supports Security Assertion Markup Language 2.0 (SAML 2.0) or OpenID Connect (OIDC) to provide an onboarding flow for your Amazon Q Business users. Such identity providers include, but aren't limited to Okta and Ping Identity.

Important

Amazon Q Business supports Microsoft Entra ID with SAML 2.0, but doesn't support OIDC for Google or Microsoft Entra ID.

With identity federation, your users get one-click access to their Amazon Q Business applications using their existing identity credentials. You also have the security benefit of identity authentication by your identity provider. You can control which users have access to Amazon Q Business using your existing identity provider.

Note

Federated groups aren't supported through IAM Federation. If you want to ingest federated groups, use the PutGroup API.

Topics

- Creating an Amazon Q Business application using IAM Federation through Okta
- Creating an Amazon Q Business application using IAM federation through Microsoft Entra ID
- Connecting multiple Amazon Q Business applications to an Identity Provider

- Making authenticated Amazon Q Business API calls using IAM federation
- Managing Amazon Q Business resources

Creating an Amazon Q Business application using IAM Federation through Okta

As the first step toward creating a generative artificial intelligence (AI) assistant, configure your external identity provider and connect it to AWS Identity and Access Management.

When you create an application environment, you can also choose to create an Amazon Q Business web experience, which your end users can use to chat with your application. You can also add subscriptions for end users who log in to your Amazon Q Business web experience using Okta. Any user logging in to your web experience is automatically provisioned with a subscription of a type that you select for them.

> **Note**
>
> As of Oct 31, 2024, once you have created a new Amazon Q Business application environment, the default web experience will allow users to interact directly with the LLM to get answers from its general knowledge or uploaded file content, even if the Admin has not yet connected any enterprise data sources.
> For existing application environments, the *Allow direct access to LLM* setting will remain as previously configured. For new application environments, the *Allow direct access to LLM* setting will be enabled by default, though Admins can still disable this if desired.

To learn more about identity federation using AWS Identity and Access Management, see the following topics:

- Identity federation in AWS on the *AWS website*.
- Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.

The following steps show how to integrate Amazon Q Business with Okta as an example. Integrating Amazon Q Business with Okta requires that you switch between tasks on the Amazon Q Business console and the Okta admin console.

Topics

- Prerequisites
- Step 1: Create and configure an Okta application
- Step 2: Add an identity provider in IAM
- Step 3: Connect IAM to Okta
- Step 4: Create Amazon Q Business application

Prerequisites

Before you start to integrate Amazon Q Business with Okta, make sure that you have:

- Created an Okta account and added at least one user with a valid email address. For more information, see Manage users on the *Okta Help Center*.
- Created IAM policies containing the permissions outlined in IAM role for an Amazon Q Business web experience using IAM Federation to:
  - Allow an Amazon Q Business web experience to invoke the API operations required to integrate your application
  - (If you're creating a Amazon Q Business default web experience) Allow Amazon Q Business to access the resources it needs to create a web experience
  - (If you're using OIDC) Allow an Amazon Q Business web experience to invoke the API operations required to decrypt the Secrets Manager secret you created for your OIDC web experience

  You will need these roles to complete creating your Amazon Q Business IAM federated application.

  > **Note**
  >
  > To create a new policy, follow the instructions in Creating IAM policies in the AWS Identity and Access Management User Guide.

- (Optional) Checked how subscriptions work for Amazon Q Business applications using IAM Federation.

Step 1: Create and configure an Okta application

This procedure outlines how to create and configure an Okta instance for an Amazon Q Business application using a built-in web experience and a custom Amazon Q Business application client you develop using Amazon Q Business APIs.

> **Important**
>
> Amazon Q Business supports Microsoft Entra ID with SAML 2.0, but doesn't support OIDC for Google or Microsoft Entra ID.

SAML

To create an Okta instance

1. Sign into Okta and go to the admin console.
2. In the left navigation pane, choose **Applications**, and then choose **Create App Integration**.
3. On the **Create a new app integration** page, choose **SAML 2.0** and then choose **Next**.
4. On the **Create SAML Integration** page, in **General Settings**, for **App name**, enter a name for the application and choose **Next**.
5. In **Configure SAML**, do the following:

    a. For **Single sign-on URL**, enter your web application endpoint.

    If you're creating a custom Amazon Q Business application, this value is the endpoint URL of your Amazon Q Business application with `/saml` added at the end. For example *`http://localhost:8000/saml`*.

    If you're creating an Amazon Q Business application generated web experience endpoint URL, this value be the Amazon Q Business generated web experience URL with `saml` added at the end. For example, *`https://abcdefgh.qbusiness.us-east-1.on.aws/saml`*.

    > **Important**
    >
    > If you're creating an Amazon Q Business application generated web experience endpoint URL, a web experience URL will be generated by Amazon Q Business after you finish creating an Amazon Q Business application. For now, enter a

placeholder URL. For example: *http://sampleurl.com*. You will update this at the end of your Amazon Q Business application creation process.

b. Deselect the **Use this for Recipient URL and Destination URL** box.

c. Then, for the **Recipient URL** field, enter the following AWS endpoint: `https://signin.aws.amazon.com/saml`.

d. For **Destination URL**, enter your web application endpoint.

If you're creating a custom Amazon Q Business application, this value is the endpoint URL of your Amazon Q Business application with `/saml` added at the end. For example *http://localhost:8000/saml*.

If you're creating an Amazon Q Business application generated web experience endpoint URL, this value be the Amazon Q Business generated web experience URL with `saml` added at the end. For example, *https://abcdefgh.qbusiness.us-east-1.on.aws/saml*.

If you're creating an Amazon Q Business application generated web experience endpoint URL, a web experience URL will be generated by Amazon Q Business after you finish creating an Amazon Q Business application. For now, enter a placeholder URL. For example: *http://sampleurl.com*. You will update this at the end of your Amazon Q Business application creation process.

e. For **Audience URI (SP Identity ID)**, enter the following AWS endpoint: `https://signin.aws.amazon.com/saml`.

f. For **Name ID format**, set to **Persistent**.

g. The, scroll down to the bottom of the page and select **Next**.

6. On the Create SAML Integration page, select the option that best fits your use case and then select **Finish**. You will be redirected to the application summary page.

7. On the application summary page, from the top navigation menu, select **Assignments**, and then select **Assign**. Then, complete the following steps:

a. To assign users to your Okta app, choose between **Assign to People** and **Assign to Groups**.

b. In the dialog box that opens up, locate the users or groups you want to assign to your application and then select **Assign**.

c. Then, choose **Done**.

8. Next, you download the SAML payload and copy your **Sign on URL**.

   You need to provide the SAML payload when you create an identity provider in IAM.

   If you choose to create a web experience from the Amazon Q Business console (Step 4 of this page), you input the **Sign on URL** or **Single Sign-On URL** (the URL where users sign in to access an application integrated with an identity provider) as the **Authentication URL**. The standard authentication URL format for Okta is: `https://<sub_domain>.okta.com/app/<app_name>/<app_id>/sso/saml`.

   From the top navigation menu of your application home page, select **Sign On**. Then, complete the following steps:

   a. In the **Settings**, from the **SAML 2.0** section, from **Metadata details** section, to copy the metadata file XML file by choosing **Copy**. Then, save it in `.xml` format.

      > **Note**
      >
      > You can also navigate to the metadata URL and copy the network response payload and paste it in a file that you save in `.xml` format.

      For more information, see Create SAML app integrations on the *Okta Help Center* website.

   b. Then, from **Sign on URL**, select the **Copy** icon to copy the Sign on URL. Save it in a text editor of your choice.

OIDC

To create an Okta instance

1. Sign into Okta and go to the admin console.
2. In the left navigation pane, choose **Applications**, and then choose **Create App Integration**.
3. On the **Create a new app integration** page, do the following:
   - Choose **OIDC – OpenID Connect**.
   - Choose **Web application**.
   - Then, choose **Next**.

4. On the **New Web App Integration** page, do the following:

   - In **General Settings**, for **App name**, enter a name for the application.
   - In **Grant type**, for **Core grants**, ensure that **Authorization Code** is selected.
   - In **Sign-in-redirect URIs**, add a URL that Okta will send the authentication response and ID token for the user's sign in request.

     If you're using a custom application, the value of this URL will be `http://localhost:8080/authorization-code/callback`, where `http://localhost:8080` is your custom web experience endpoint URL.

     If you're creating an Amazon Q Business application generated web experience endpoint URL, this value will be the Amazon Q Business generated web experience URL with `/authorization-code/callback` added at the end. Amazon Q Business generates this web experience URL when you create a Amazon Q Business application using in Step 4. For now, enter a placeholder URL. For example: *`http://sampleurl.com/authorization-code/callback`*. You will update this after you finish creating a Amazon Q Business application by inputting your Amazon Q Business web experience URL with `/authorization-code/callback` added at the end. For example, `https://abcdefgh.qbusiness.us-east-1.on.aws/authorization-code/callback`.
   - In **Assignments**, select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.
   - Then, select **Save**.

5. From the application summary page, from **General**, do the following:

   - From **Client Credentials**, copy and save the **Client ID**. You will input this as the **Audience** when you create an identity provider in AWS Identity and Access Management in the next step.
   - From **CLIENT SECRETS**, copy and save the **Secret**. If you choose to use an Amazon Q Business default web experience, you will need to input this in an Secrets Manager secret when you configure **Web experience settings** in the Amazon Q Business console.

6. From the left navigation menu, select **Security**, and then select **API**.
7. Then, from **Authorization Servers**, do the following:

- Copy the **Issuer URI**, for example `https://trial-okta-instance-id.okta.com/oauth2/default`. You will need to input this value as the **Provider URL** when you add your identity provider in IAM in Step 2.
- Select **default**, and then select **Claims**.

8. In **Claims**, select **Add claim**, and then do the following:

- For **Name**, add `https://aws.amazon.com/tags`.
- For **Include in token type**, choose `ID token` and select **Always**.
- For Okta, the **Value** will be the following: `{"principal_tags": {"Email": {user.email} }}`. For other identity providers, use a valid JSON object in the following format:

```
"principal_tags": {
    "Email": [email]
}
```

> **Note**
>
> To activate Amazon Q Business response personalization for your application, add the following optional tags: `{"principal_tags": {"Email": {user.email}, "country": {user.city != null ? user.city : ""}}}`. Ensure that null values aren't passed via principal tags by using the operation `user.$attribute != null ? user.$attribute : ""`.

- For **Include in**, choose `Any scope`.
- Select **Create**.

You are now ready to go to the AWS Identity and Access Management console and create an OIDC identity provider instance.

> **Important**
>
> Amazon Q Business supports Microsoft Entra ID with SAML 2.0, but doesn't support OIDC for Google or Microsoft Entra ID.

You are now ready to move to the AWS Identity and Access Management console to create an identity provider integration for your Okta instance.

Step 2: Add an identity provider in IAM

In this step, you add configure AWS Identity and Access Management by creating an identity provider integration for your Okta instance.

SAML

To connect Okta to AWS Identity and Access Management

1. Sign in to the AWS Identity and Access Management console.
2. In the left navigation menu, from **Access management**, select **Identity providers**.
3. From **Identity providers**, select **Add provider**.
4. In **Add an identity provider**, for **Configure provider** do the following:
   - For **Provider type** – Select **SAML**.
   - For **Provider name** – Add a name to identify your identity provider.
   - For **Metadata document** – Upload the `.xml` file you downloaded and saved from Okta in Step 1.
   - For **Add tags - *optional*** – Add tags to resources to help identify, organize, or search for the identity provider you're adding.
   - Select **Add provider**.
5. On the **Identity provider** summary page, from **Provider**, select the provider you just added do the following:
   - From **Summary** copy the **ARN** and save the value. You will need it when you add your trust policy and when you connect your AWS Identity and Access Management identity provider to your Okta instance. The format of the ARN is: `arn:aws:iam::`*`aws-account-id`*`:saml-provider/`*`assigned-iam-idp-name`*.
   - Then, select **Assign role** to create an IAM role with the necessary permissions for your identity provider.
6. In **Assign role**, for **Role options** select **Create a new role**.
7. Then, on the **Selected trusted entity** page, do the following:
   - For **Trusted entity type** select **SAML 2.0 federation**.

- In **SAML 2.0 federation**, from the **SAML 2.0-based provider** drop-down, select the identity provider you added.
- For **Access to be allowed**, select **Allow programmatic access only**.
- For **Attribute**, select **SAML:aud**.
- For **Value**, enter the following: `https://signin.aws.amazon.com/saml`.
- Select **Next**.

8. On the **Add permissions** page, for **Permissions policies** choose an IAM policy with the required permissions and then select **Next**.

   For the policy permissions required, see IAM role for an Amazon Q Business web experience using IAM Federation.

   > **Note**
   >
   > To create a new policy, follow the instructions in Creating IAM policies in the AWS Identity and Access Management User Guide.

9. In the **Name, review, and create** page, add a **Role name**, and optional role description and tags to identify your IAM role. Then, select **Create role**.
10. From the **Roles** page, select the IAM role you just created. Then, from the role summary page, do the following:

    - Copy the role **ARN** and save it. You will need this information to connect your AWS Identity and Access Management identity provider instance to Okta. The format of the ARN will be like this: `arn:aws:iam::111122223333:role/sample-role`.
    - In **Trust relationships**, select **Edit trust policy** and select **Add new statement** to add the following trust policy, replacing the value for *`account_id`* with your AWS account ID and *`saml_provider`* with the *`assigned-iam-idp-name`* you copied from your IAM identity provider ARN you copied:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": "sts:AssumeRoleWithSAML",
            "Sid": "SAMLAssumeRoleAccess",
            "Effect": "Allow",
```

```
            "Condition": {
                "StringEquals": {
                    "SAML:aud": "https://signin.aws.amazon.com/saml"
                }
            },
            "Principal": {
                "Federated": "arn:aws:iam::111122223333:saml-provider/saml-
provider-name"
            }
        },
        {
            "Action": "sts:TagSession",
            "Sid": "SAMLTagSessionAccess",
            "Effect": "Allow",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/Email": "*"
                }
            },
            "Principal": {
                "Federated": "arn:aws:iam::111122223333:saml-provider/saml-
provider-name"
            }
        }
    ]
}
```

- Then, select **Update policy**.

You are now ready to return to Okta to complete the process of establishing a trust relationship between AWS Identity and Access Management and Okta.

OIDC

To connect Okta to AWS Identity and Access Management

1. Sign in to the AWS Identity and Access Management console.
2. In the left navigation menu, from **Access management**, select **Identity providers**.
3. From **Identity providers**, select **Add provider**.
4. In **Add an identity provider**, for **Configure provider** do the following:

   - For **Provider type** – Select **OpenID Connect**.

- For **Provider URL** – Paste the **Input URI** you copied from the Okta console. For example, `trial-okta-instance-id.okta.com/oauth2/default`.
- For **Audience** – Copy and paste the Client ID you copied from Okta from the Okta console.
- For **Add tags - *optional*** – Add tags to resources to help identify, organize, or search for the identity provider you're adding.
- Select **Add provider**.

5. On the **Identity provider** summary page, from **Provider**, select the provider you added do the following:

   - From **Summary** copy the **ARN** and save the value. You will need it when you add your trust policy and when you connect your AWS Identity and Access Management identity provider to your Okta instance. The format of the ARN is: `arn:aws:iam::aws-account-id:oidc-provider/issuer`.
   - Then, select **Assign role** to create an IAM role with the necessary permissions for your identity provider.

6. In the **Assign role** dialog box that opens, for **Role options** select **Create a new role**.
7. Then, on the **Selected trusted entity** page, do the following:

   - For **Trusted entity type** select **Web identity**.
   - In **Web identity**, from the **Identity provider** drop-down, select the identity provider you added.
   - For **Audience**, select your Client ID.
   - Select **Next**.

8. On the **Add permissions** page, for **Permissions policies** choose an IAM policy to add, and then select **Next**. You can add an existing policy or update your policy you're creating to include required permissions. Your policy must contain the permissions outlined in IAM role for an Amazon Q Business web experience using IAM Federation.

   > **Note**
   >
   > To create a new policy, follow the instructions in Creating IAM policies in the AWS Identity and Access Management User Guide.

9. In the **Name, review, and create** page, add a **Role name** add a role name, and optional role description and tags to identify your IAM role. Then, select **Create role**.
10. From the **Roles** page find and select the IAM role you created. Then, from the role summary page, in **Trust relationships**, select **Edit trust policy** and select **Add new statement**
11. Then, add the following statement to your existing trust policy, replacing *`account-id`* with your AWS account ID, *`clientId`* with the OIDC client ID you copied, and *`iss`* with the *`issuer`* value from your IAM identity provider ARN:

    ```
    ```

12. Then, select **Update policy**.

Now, move on to the Amazon Q Business console to create your application.

Step 3: Connect IAM to Okta

In this step, you complete configuring the trust relationship between AWS Identity and Access Management and Okta.

SAML

1. Sign into Okta and go to the admin console.
2. In the left navigation pane, choose **Applications**, and then choose the Okta application you created.
3. In **General**, from **SAML Settings** choose **Edit**.
4. In **Edit SAML**, for **General Settings** choose **Next**.
5. In **Configure SAML**, scroll down to the **Attribute Statements** section, and add the following attributes:

   Attribute 1

   - For the **Name** field, provide the following for the email attribute: `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`.
   - For the **Name format** field, keep it set to **Unspecified**.

- For the **Value** field, provide a mapping to the attribute by selecting `user.email` from the drop-down list.

> **Note**
>
> You can add more attributes to enable Amazon Q Business response personalization. To do this, provide the following value for the **Name** field: `https://aws.amazon.com/SAML/Attributes/PrincipalTag:<attributeName>`. Keep the **Name format** field **Unspecified**. For **Value**, provide an attribute mapping by selecting a user attribute like `user.city` from the drop-down list.

Attribute 2

- For the **Name** field, provide the following name for the role attribute: `https://aws.amazon.com/SAML/Attributes/Role` .
- For the **Name format** field, keep it set to **Unspecified**.
- For the **Value** field, add a mapping to the attribute in the following format using the values you copied from Step 2 of this section: `IAMroleArn,IAMidpArn`. For example: `arn:aws:iam::111122223333:role/sample-role,arn:aws:iam::111122223333:saml-provider/okta-idp`.

Attribute 3

- Then, for the **Name** field, provide the following name for the role session name attribute: `https://aws.amazon.com/SAML/Attributes/RoleSessionName`.
- For the **Name format** field, keep it set to **Unspecified**.
- For the **Value** field, provide a mapping to the attribute by selecting `user.email` from the drop-down list.
- Choose **Next**, and then choose **Finish**.

Now, move on to the Amazon Q Business console to create your application.

OIDC

This step isn't needed for OIDC.

Step 4: Create Amazon Q Business application

To create an Amazon Q Business application environment, you can use either the AWS Management Console or the Amazon Q Business API. When you create an application, response generation from large language model (LLM) knowledge is enabled by default.

If you're using an Amazon Q Business default web experience for your application, you can choose to generate it in this step. If you're using this generated URL as your web experience endpoint, you need to return to Okta to update your identity provider instance with this information.

You also add subscriptions for end users logging into your Amazon Q Business web experience using Okta. Any user logging into your web experience is automatically provisioned a subscription of the type you select.

> **Warning**
>
> User subscriptions are connected to the AWS account Amazon Q Business applications are attached to. If the same user logs in to an Amazon Q Business application using multiple AWS accounts, they're charged multiple times. Create an Amazon Q Business application using IAM Identity Center for user management to avoid this issue.

For a consolidated view of your user subscriptions—including a list of subscribed users, their subscription status, and applications, accounts, or services a user can access through their subscriptions—see the Amazon Q subscriptions page. Subscriptions can only be viewed centrally and *not* be created or updated from the Amazon Q subscription management console.

For more information on user subscriptions for an IAM federated Amazon Q Business application, see Subscriptions for applications using IAM Federation.

As a prerequisite, make sure that you complete the setting up tasks. If you're using the AWS CLI or the API, make sure that you created the required IAM roles.

The following tabs provide a procedure for creating your Amazon Q Business application environment using the AWS Management Console and code examples for using the AWS CLI.

Console

To create an application

1. Sign in to the AWS Management Console and open the Amazon Q Business console.

2. On the **Create application** page, for **What kind of application do you want to create?**, enter the following information for your Amazon Q Business application:

   a. **Application name** – A name for your Amazon Q Business application environment for easy identification. This name is only visible in the AWS Management Console. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters. Amazon Q Business auto-generates an application name for you, unless you choose to enter a custom name.

   b. **Outcome** – Select **Web experience** to create a web experience for your application. Amazon Q Business creates a web experience by default when you create an application. If you don't want to create a web experience, deselect this option.

3. For **Access management method**, choose **AWS IAM Identity Provider**.

   Then, for **Choose an identity provider type**, choose between **Security Assertion Markup Language (SAML)** and **OpenID Connect (OIDC)**.

   a. For **SAML**, do the following:

      i. For **Select Identity Provider**, choose the identity provider you've created in AWS Identity and Access Management to use with your Amazon Q Business application.

      ii. For **Authentication URL**, provide the authentication URL for Okta. Your authentication URL must be of the following format: `https://<sub_domain>.okta.com/app/<app_name>/<app_id>/sso/saml`. Enter the **Sign on URL** you copied in Step 1.

      When end users navigate to the web experience URL they're redirected to this authentication URL where they provide their login ID and password. After successful authentication, they're redirected back to the web experience URL to begin chatting.

   b. For **OIDC**, do the following:

      i. For **Select Identity Provider**, choose the identity provider you've created in AWS Identity and Access Management to use with your Amazon Q Business application.

      ii. For **ClientID for OIDC**, input the OIDC client ID you copied in Step 1.

      iii. For **AWS Secrets Manager**, choose to create a new Secrets Manager secret or add an existing one to allow Amazon Q Business to access your Okta instance. Your secret must contain the client secret you copied from your Okta instance.

iv. In **Choose method to authorize Amazon Q Business web experience to use Secrets**, choose an existing IAM role to allow your Amazon Q Business web experience to access the AWS resources it needs to function.

For the policy permissions required, see IAM role for an Amazon Q Business web experience using IAM Federation.

> **Note**
>
> To create a new policy, follow the instructions in Creating IAM policies in the AWS Identity and Access Management User Guide.

4. For **Default subscription settings**, for **Subscription tier**, choose between **Q Business Pro** and **Q Business Lite**. Any user logging in to your web experience will be assigned this subscription type by default.
5. For **Application details** – Amazon Q Business chooses the following configuration settings for your application by default:

   a. For **Application service access** – Amazon Q Business will create a new service-linked role for your application.

   b. **Encryption** – Amazon Q Business will create an AWS owned AWS KMS key to encrypt your data.

   c. For **Web experience service access** – If you've chosen to create a web experience, Amazon Q Business requires you select an existing role to allow end users to log in to a Amazon Q Business web experience.

6. (Optional) To customize **Application details**, expand the **Application details section**, and then do the following:

   a. In **Application service access**, for **Choose a method to authorize Amazon Q Business**, choose from the following options:

      i. **Create and use a new service-linked role (SLR)** – Create and use a new Amazon Q Business-managed IAM role to allow it to access the AWS resources it needs to create your application.

      ii. **Create and use a new service role (SR)** – Create and use a new IAM role for Amazon Q Business to allow it to access the AWS resources it needs to create your application.

iii. **Use an existing service role (SR)/service-linked role (SLR)** – Use an existing service role or service-linked IAM role to allow Amazon Q Business to access the AWS resources it needs to create your application.

> **Note**
>
> For more information about example service roles, see IAM role for an Amazon Q Business application. For information on service-linked roles, including to manage them, see Using service-linked roles.

iv. **Service role name** – A name for the service (IAM) role you created for easy identification on the console.

b. For **Encryption** – Amazon Q Business encrypts your data by default using AWS managed AWS KMS keys. To customize your encryption settings, select **Customize encryption settings (advanced)**. Then, you can choose to use an existing AWS KMS key or create a new one.

c. In **Web experience service access**, enter the following information:

i. For **Choose a method to authorize Amazon Q Business** – A service access role assumed by end users when they sign in to your web experience that grants them permission to start and manage conversations Amazon Q Business. You can only choose to use an existing role. For more information on how to create a role and permissions needed, see Prerequisites for creating an IAM federated application.

ii. **Service role name** – A name for the service role you created for easy identification on the console.

7. To start creating your application, choose **Create**.

> **Note**
>
> If you're creating a web experience, you can also choose to create your application and view your web experience by selecting **Create and open web experience**.

8. Once the application creation process completes, the web experience settings section on your application summary page will display your Amazon Q Business web experience URL. Copy the URL to a file and then, depending on the authentication type you've chosen, do the following:

a. **If you're using SAML** – Add `/saml` at the end of the URL. Then, Return to the Okta console, edit your SAML application to update **Single sign-on URL** and **Destination URL** you added in Step 1 to your web experience URL. Remember to save your changes.

b. **If you're using OIDC** – Add `/authorization-code/callback` at the end of the URL. Then, return to the Okta console to edit your OIDC application and update the **Sign-in-redirect URI** value you added in Step 1. Remember to save your changes.

AWS CLI

To configure an Amazon Q Business application

```
aws qbusiness create-application \
--display-name application-name \
--iam-identity-provider-arn iam-identity-provider-arn \
--client-id-for-oidc client-id-for-oidc \
--identity-type identity-type\
--role-arn roleArn \
--description application-description \
--encryption-configuration kmsKeyId=<kms-key-id> \
--attachments-configuration attachmentsControlMode=ENABLED
```

You've finished configuring your Amazon Q Business application. Your authenticated end users can now log in and chat with your web experience.

Creating an Amazon Q Business application using IAM federation through Microsoft Entra ID

As the first step toward creating a generative artificial intelligence (AI) assistant, configure your external identity provider and connect it to AWS Identity and Access Management.

When you create an application environment, you can also choose to create an Amazon Q Business web experience, which your end users can use to chat with your application. You can add subscriptions for end users who log in to your Amazon Q Business web experience using Microsoft Entra ID. Any user logging in to your web experience is automatically provisioned with a subscription of a type that you select for them.

> **Note**
>
> As of Oct 31, 2024, once you have created a new Amazon Q Business application environment, the default web experience will allow users to interact directly with the LLM to get answers from its general knowledge or uploaded file content, even if the Admin has not yet connected any enterprise data sources.
> For existing application environments, the *Allow direct access to LLM* setting will remain as previously configured. For new application environments, the *Allow direct access to LLM* setting will be enabled by default, though Admins can still disable this if desired.

To learn more about identity federation using AWS Identity and Access Management, see the following topics:

- Identity federation in AWS on the *AWS website*.
- Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.

The following steps show how to integrate Amazon Q Business with Microsoft Entra ID. Integrating Amazon Q Business with Microsoft Entra ID requires that you switch between tasks on the Amazon Q Business console and the Microsoft Entra ID admin portal.

Topics

- Prerequisites
- Step 1: Create and configure a Microsoft Entra ID application
- Step 2: Create an IAM identity provider
- Step 3: Update your Microsoft Entra ID application with the IAM role ARN
- Step 4: Create an Amazon Q Business application
- Step 5: Update your Microsoft Entra ID application with the web experience URL
- Troubleshooting Microsoft Entra ID integration

Prerequisites

Before you start to integrate Amazon Q Business with Microsoft Entra ID, make sure that you have:

- Created a Microsoft Entra ID account and added at least one user with a valid email address. For more information, see Add users in Microsoft Entra ID on the *Microsoft Learn website*.
- Appropriate permissions in Microsoft Entra ID to create and configure enterprise applications. Review the Microsoft Entra ID built-in roles documentation to ensure you have the required permissions. Typically, you need the `Application Administrator` or `Cloud Application Administrator` role.
- Created IAM policies containing the permissions outlined in IAM role for an Amazon Q Business web experience using IAM Federation to:
  - Allow an Amazon Q Business web experience to invoke the API operations required to integrate your application
  - **(If you're creating a Amazon Q Business default web experience)** Allow Amazon Q Business to access the resources it needs to create a web experience

  You will need these roles to complete creating your Amazon Q Business IAM federated application.

  > **Note**
  >
  > To create a new policy, follow the instructions in Creating IAM policies in the AWS Identity and Access Management User Guide.

- (Optional) Checked how subscriptions work for Amazon Q Business applications using IAM Federation.

Step 1: Create and configure a Microsoft Entra ID application

This procedure outlines how to create and configure a Microsoft Entra ID instance for an Amazon Q Business application using a built-in web experience and a custom Amazon Q Business application client you develop using Amazon Q Business APIs.

> **Important**
>
> Amazon Q Business supports Microsoft Entra ID with SAML 2.0 only. OIDC is not supported for Microsoft Entra ID.

To create a Microsoft Entra ID instance

1. Sign into the Microsoft Entra admin center in your Microsoft Azure Portal.
2. In the left navigation pane, choose **Enterprise apps**.
3. From **All applications**, choose **+ New application** from the top navigation pane.
4. On the **Browse Microsoft Entra gallery** page, choose **Amazon Web Services (AWS)**, and then select **AWS Single-Account Access**.
5. Then, in the **AWS Single-Account Access** menu that opens, in **Name**, add a name for your application. For example: *QBusinessSAMLProvider*. Then, select **Create**.
6. When the application is ready, on the **Overview** page of your application, from **Getting Started** choose **Single sign-on**.
7. On the **Single sign-on** page, for **Select a single sign-on method**, select **SAML**.

   Selecting SAML configures the application to use Security Assertion Markup Language (SAML) 2.0 for authentication, which is the protocol required for IAM federation with AWS services like Amazon Q Business.
8. On the **Set up Single Sign-On with SAML** page, for **Basic SAML Configuration**, choose **Edit**, and then configure the following settings:

   - For **Identifier (Entity ID)**, enter your web application endpoint.

     If you're creating an Amazon Q Business application generated web experience endpoint URL, this value be the Amazon Q Business generated web experience URL with `saml` added at the end. For example, *https://abcdefgh.qbusiness.us-east-1.on.aws/saml*. The web experience URL will be generated by Amazon Q Business after you finish creating an Amazon Q Business application. For now, enter a placeholder URL. For example: *https://sampleurl.com*. You will update this at the end of your Amazon Q Business application creation process.
   - For **Reply URL (Assertion Consumer Service URL)** – Enter your web application endpoint.

     If you're creating an Amazon Q Business application generated web experience endpoint URL, this value be the Amazon Q Business generated web experience URL with `saml` added at the end. For example, *https://abcdefgh.qbusiness.us-east-1.on.aws/saml*. The web experience URL will be generated by Amazon Q Business after you finish creating an Amazon Q Business application. For now, enter a placeholder URL. For example:

https://sampleurl.com. You will update this at the end of your Amazon Q Business application creation process.

- Select **Save**.

9. In the **SAML Certificates** section, download the **Federation Metadata XML** file. You will need this file when you create an identity provider in IAM.

   The **Federation Metadata XML** file contains all the necessary SAML metadata that IAM needs to establish trust with your Microsoft Entra ID application, including certificate information, entity IDs, and endpoint URLs. This file will be uploaded to IAM when creating the identity provider in the next step.

You're now ready to move on to configuring AWS Identity and Access Management on the AWS Management Console.

Step 2: Create an IAM identity provider

After you create and configure your Microsoft Entra ID application, create an IAM identity provider.

To connect Microsoft Entra ID to AWS Identity and Access Management

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management.
2. In the navigation pane, choose **Identity providers**, and then choose **Add provider**.
3. For **Configure provider**, do the following:

   a. For **Provider type**, choose **SAML**.

   b. For **Provider name**, enter a name for your identity provider (for example, *EntraIDProvider*).

   c. For **Metadata document**, choose **Choose file** and upload the **Federation Metadata XML** file that you downloaded from Microsoft Entra ID.

   d. Choose **Add provider**.

4. On the **Identity provider** summary page, from **Provider**, select the provider you just added do the following:

   - From **Summary** copy the **ARN** and save the value. You will need it when you add your IAM trust policy and when you connect your AWS Identity and Access Management identity provider to your Microsoft Entra ID instance. The format of the ARN is: `arn:aws:iam::`*aws-account-id*`:saml-provider/`*assigned-iam-idp-name*.

- Then, select **Assign role** to create an IAM role with the necessary permissions for your identity provider.

5. In **Assign role**, for **Role options** select **Create a new role**.
6. Then, on the **Selected trusted entity** page, do the following:

   - For **Trusted entity type** select **Custom trust policy**.
   - In **Custom trust policy**, add the following trust policy, replacing the value for *`AWS IAM Identity Provider ARN`* with the identity provider ARN you copied in the previous step:

     > **Note**
     >
     > Leave the `SAML:aud` field as *`https://sampleurl.com`* for now. You'll come back to update it with your Amazon Q web experience URL as part of Step 5 of this tutorial.

     Select **Next**.

7. On the **Add permissions** page, for **Permissions policies** choose an IAM policy with the required permissions and then select **Next**.

   For the policy permissions required, see IAM role for an Amazon Q Business web experience using IAM Federation. Optionally, select **AdministratorAccess**.

   > **Note**
   >
   > To create a new policy, follow the instructions in Creating IAM policies in the AWS Identity and Access Management User Guide.

8. In the **Name, review, and create** page, add a **Role name**, and optional role description and tags to identify your IAM role. Then, select **Create role**.
9. From the **Roles** page, select the IAM role you just created. Then, from the role summary page, do the following:

- Copy the role **ARN** and save it. You will need this information to connect your AWS Identity and Access Management identity provider instance to Microsoft Entra ID. The format of the ARN will be like this: `arn:aws:iam::111122223333:role/sample-role`.

You are now ready to return to Microsoft Entra ID to complete the process of establishing a trust relationship between AWS Identity and Access Management and Microsoft Entra ID.

Step 3: Update your Microsoft Entra ID application with the IAM role ARN

In this step, you complete configuring the trust relationship between AWS Identity and Access Management and Microsoft Entra ID.

To update your Microsoft Entra ID application

1. Return to the Microsoft Azure Portal and navigate to the application you created.
2. In the left navigation pane, choose **Single sign-on**, then choose **Manage**. Then, choose **Single sign-on**.
3. In **Single sign-on** section, choose **Attributes & Claims**, and select **Edit**.
4. From **Required claim**, select **Unique User Identifier (Name ID)**.
5. In **Manage claim**, do the following:
   - For **Name identifier format**, choose **Persistent**.
   - For **Source attribute**, choose **user.objectid**.
   - Select **Save**.
6. Then, from **Attributes & Claims** select **Add new claim**, and in **Manage claim**, do the following:
   - For **Name** – Type **PrincipalTag:Email**.
   - For **Namespace**, type **https://aws.amazon.com/SAML/Attributes**.
   - Leave **Source** value as **Attribute**.
   - For **Source attribute**, choose **user.mail**.
   - Select **Save**.
7. Then, from your application menu, choose **Manage** and then select **Security**.
8. From **Security**, select **Permissions**.

9. In **Permissions**, choose **Application registration**.
10. From **Application registration** from the left navigation menu, select **App roles**, and then select **Create app role**. In the **Create app role** dialog box that opens, and do the following:
    - For **Display name**, add a name for your role.
    - For **Allowed member types**, choose **Both (Users/Groups + Applications)**.
    - For the **Value** field, add a mapping to the attribute in the following format using the values you copied from Step 2 of this section: `IAMroleArn,IAMidpArn`. For example: `arn:aws:iam::111122223333:role/sample-role,arn:aws:iam::111122223333:saml-provider/entra-idp`.
    - For **Description**, add a description for your app role.
    - Select **Apply**.
11. Then, in the left navigation pane of your application, choose **Users and groups**, and do the following steps.
    a. Choose **+ Add user/group** and select the users or groups you want to assign to your application, and then choose **Select**.
    b. Choose **Assign**.
12. Refresh your page. Then, from the left navigation pane of your application, choose **Manage**. Then, select **API Permissions**, and **Add a permission**.
13. In **Add a permission**. Then, on the **Request API permissions** section, do the following:
    a. Choose **APIs my organization uses** and select and open the Entra ID application you created.
    b. For **What type pf permissions does your application require?** – Choose **Application permissions**.
    c. In **Permissions** – Choose the app role permissions you created in the last step.
    d. Select **Add permissions**.
14. Then, from **Manage**, select **Properties** and copy and save the **User access URL** value for your application.

    You will need this value to create your Amazon Q application.

Your Entra ID setup is complete. You're now ready to begin creating your Amazon Q Business application.

Step 4: Create an Amazon Q Business application

After you configure Microsoft Entra ID and IAM, create an Amazon Q Business application.

To create an Amazon Q Business application

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In the navigation pane, choose **Applications**, and then choose **Create application**.
3. On the **Create application** page, for **What kind of application do you want to create?**, enter the following information for your Amazon Q Business application:

   a. **Application name** – A name for your Amazon Q Business application environment for easy identification. This name is only visible in the AWS Management Console. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters. Amazon Q Business auto-generates an application name for you, unless you choose to enter a custom name.

   b. For **User access**, choose **Authenticated access**.

   c. For **Outcome**, choose **Web experience**.
4. For **Access management method**, choose **AWS IAM Identity Provider**.

   Then, for **Choose an identity provider type**, choose **Security Assertion Markup Language (SAML)**.

   For **SAML**, do the following:

   a. For **Select Identity Provider**, choose the identity provider you've created in AWS Identity and Access Management to use with your Amazon Q Business application.

   b. For **Authentication URL**, provide the authentication URL for Entra ID. Your authentication URL must be of the following format: `https://myapps.microsoft.com/signin/app_name/user_access_url_suffix`.

      For the `user_access_url_suffix`, copy the value of everything after `https://myapps.microsoft.com/signin/` from the **User access URL** you copied and saved in the last step.

      When end users navigate to the web experience URL they're redirected to this authentication URL where they provide their login ID and password. After successful authentication, they're redirected back to the web experience URL to begin chatting.

5. For **Default subscription settings**, for **Subscription tier**, choose between **Q Business Pro** and **Q Business Lite**. Any user logging in to your web experience will be assigned this subscription type by default.
6. For **Application details** – Amazon Q Business chooses the following configuration settings for your application by default:

   a. For **Application service access** – Amazon Q Business will create a new service-linked role for your application.

   b. **Encryption** – Amazon Q Business will create an AWS owned AWS KMS key to encrypt your data.

   c. For **Web experience service access** – If you've chosen to create a web experience, Amazon Q Business requires you select an existing role to allow end users to log in to a Amazon Q Business web experience.
7. (Optional) To customize **Application details**, expand the **Application details section**, and then do the following:

   a. In **Application service access**, for **Choose a method to authorize Amazon Q Business**, choose from the following options:

      i. **Create and use a new service-linked role (SLR)** – Create and use a new Amazon Q Business-managed IAM role to allow it to access the AWS resources it needs to create your application.

      ii. **Create and use a new service role (SR)** – Create and use a new IAM role for Amazon Q Business to allow it to access the AWS resources it needs to create your application.

      For **Service role name** – A name for the service (IAM) role you created for easy identification on the console.

      iii. **Use an existing service role (SR)/service-linked role (SLR)** – Use an existing service role or service-linked IAM role to allow Amazon Q Business to access the AWS resources it needs to create your application.

> **Note**
>
> For more information about example service roles, see IAM role for an Amazon Q Business application. For information on service-linked roles, including to manage them, see Using service-linked roles.

b. For **Encryption** – Amazon Q Business encrypts your data by default using AWS managed AWS KMS keys. To customize your encryption settings, select **Customize encryption settings (advanced)**. Then, you can choose to use an existing AWS KMS key or create a new one.

c. In **Web experience service access**, enter the following information:

- For **Choose a method to authorize Amazon Q Business** – A service access role assumed by end users when they sign in to your web experience that grants them permission to start and manage conversations Amazon Q Business. Choose the IAM role you created in Step 2.

8. To start creating your application, choose **Create**.

> **Note**
>
> If you're creating a web experience, you can also choose to create your application and view your web experience by selecting **Create and open web experience**.

9. Once the application creation process completes, the web experience settings section on your application summary page will display your Amazon Q Business web experience URL. Copy the URL to a file and add `/saml` at the end of the web experience URL.

10. Then, open IAM on the AWS Management Console, and do the following:

a. From the left navigation menu, for **Access management**, choose **Roles**, and then choose the IAM role you created in Step 2 of this tutorial.

b. From the role summary page, select **Trust relationships**, and then select **Edit trust policy**.

c. Replace the placeholder *`{{https://sampleurl.com}}`* with the Amazon Q web application URL you copied in the previous step.

d. Select **Update policy**.

You've finished configuring your Amazon Q Business application. You're now ready to return to Entra ID to make the final changes needed to successfully launch your web experience application.

Step 5: Update your Microsoft Entra ID application with the web experience URL

After you create your Amazon Q Business application and web experience, update your Microsoft Entra ID application with the web experience URL.

Return to the Entra ID console, edit the Basic SAML Configuration of your Entra ID application to update the **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** you added in Step 1 to your web experience URL. Remember to save your changes.

To update your Microsoft Entra ID application

1. Return to the Microsoft Entra admin center and navigate to your application.
2. In the left navigation pane, choose **Single sign-on**.
3. In the **Basic SAML Configuration** section, choose **Edit**.
4. Update the following fields with your Amazon Q Business web experience URL:
    a. For **Identifier (Entity ID)**,replace *https://sampleurl.com* with your web experience URL with the `/saml` suffix added. For example: *https://abcdefgh.qbusiness.us-east-1.on.aws/saml*.
    b. For **Reply URL (Assertion Consumer Service URL)**, replace *https://sampleurl.com* with your web experience URL with `/saml` added at the end. For example: *https://abcdefgh.qbusiness.us-east-1.on.aws/saml*.
5. Choose **Save**.

You've finished configuring your Amazon Q Business for chat. Your authenticated end users can now log in and chat with your web experience.

Troubleshooting Microsoft Entra ID integration

If you encounter issues with your Microsoft Entra ID integration, check the following:

SAML assertion validation errors

If you receive errors about invalid SAML assertions, verify that:

- The **Identifier (Entity ID)** is set to `https://signin.aws.amazon.com/saml`.

- The **Reply URL** ends with `/saml` and matches your web experience URL exactly.
- All three required SAML attributes are correctly configured: `Role`, `RoleSessionName`, and `PrincipalTag:Email`.

Access denied errors

If users receive access denied errors when trying to access the Amazon Q Business web experience, check that:

- The IAM role ARN and identity provider ARN in the `Role` attribute are correct and separated by a comma.
- The IAM role has the necessary permissions for Amazon Q Business web experience access.
- The trust relationship in the IAM role is correctly configured to trust the SAML identity provider.

User not provisioned errors

If users receive errors about not being provisioned in Amazon Q Business, verify that:

- The `PrincipalTag:Email` attribute is correctly configured to use `user.mail`.
- The user has a valid email address in Microsoft Entra ID.
- The default subscription tier is correctly set in the Amazon Q Business application.

Testing SAML configuration

To test your SAML configuration:

1. In the Microsoft Entra admin center, navigate to your application.
2. Choose **Single sign-on**, then scroll down to **Test single sign-on with <application name>**.
3. Choose **Test** to sign in as the current user, or choose **Test as another user** to sign in as a different user.
4. If the test is successful, you'll be redirected to your Amazon Q Business web experience.

For SAML assertion validation errors, access denied errors, and user not provisioned errors, you'll need to check the Microsoft Entra ID configuration in the admin portal as described in the Console tab.

For more information about SAML federation with Microsoft Entra ID, see Set up SAML-based single sign-on in the Microsoft Entra documentation.

Connecting multiple Amazon Q Business applications to an Identity Provider

You can connect multiple Amazon Q Business custom applications to a single SAML 2.0 or OIDC based identity provider (IdP) application. Connecting multiple Amazon Q Business applications to a single identity provider enables end users access Amazon Q Business with all their web-based tools and services through a single sign-on (SSO) provided by the IdP.

Most IdPs allow you to configure additional custom web applications alongside existing ones. In this section we use Okta as an example to show you the specific steps to configure a new custom application.

> **Important**
>
> Amazon Q Business supports Microsoft Entra ID with SAML 2.0, but doesn't support OIDC for Google or Microsoft Entra ID.

Topics

- Using SAML
- Using OIDC

Using SAML

In this section we use Okta as an example to show you the specific steps to configure a new custom application using SAML 2.0.

To connect multiple Amazon Q Business custom applications to Okta

1. Sign into Okta and go to the admin console.
2. In the left navigation pane, choose **Applications**, and then choose your existing SAML 2.0 application.
3. From **General**, choose **SAML settings**.
4. Keep your **General Settings** as is and select **Next**.

5. In **Edit SAML Integration**, for **SAML Settings**, under **General**, make sure you've already entered the **Single sign-on URL** and **Audience URI** for your first SAML application. For steps on how to do this, see Create and configure an Okta application.
6. Then, from **General**, select **Show Advanced Settings**.
7. Scroll down to **Other Requestable SSO URLs** and select **Add Another**.
8. Then, add a **Single sign-on URL** for each additional SAML application you want to configure, and provide an index value for each. Example URL format: *http://localhost:8000/saml*.
9. Then, scroll down and select **Next**.
10. On the **Feedback** page, select **Finish**.

You're done with setting up your Okta application for multiple Amazon Q Business applications.

To make a request to this URI, you need to construct a SAML request in the following format:

```
<samlp:AuthnRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="_uniqueID12345"
    Version="2.0"
    IssueInstant="2024-08-08T12:00:00Z"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
    Destination="https://idp-sso-url/sso"
    AssertionConsumerServiceIndex="0"
    <saml:Issuer>https://sp.example.com/</saml:Issuer>
    <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
 AllowCreate="true"
</samlp:AuthnRequest>
```

Then, you send a SAML request to your to your custom web application's URI with index 0. The SAML request is usually sent via HTTP redirect, which requires the XML to be Base64 encoded. This can be done programmatically in various languages. For example, in JavaScript, you would do the following:

```
const samlRequest = '<samlp:AuthnRequest ...>...</samlp:AuthnRequest>'; // Your SAML
 request
const encodedRequest = btoa(samlRequest); // Base64 encoding
```

After encoding, redirect the user to the IdP with the following SAML request as parameter:

```
window.location.href = `https://idp.example.com/sso?SAMLRequest=$${encodedRequest}`;
```

Using OIDC

You can configure multiple redirect URLs for a single OpenID Connect (OIDC) application. In this section we use Okta as an example to show you the specific steps to configure a new custom application using OIDC.

To connect multiple Amazon Q Business custom applications to Okta

1. Sign into Okta and go to the admin console.
2. From **General**, scroll down to **General Settings**, and then select **Edit**.
3. From **LOGIN**, for **Sign-in redirect URIs**, and then select **Edit**.
4. In **Sign-in redirect URIs**, choose **Add URI** to add multiple URIs. Then, select **Save**.

You're done with setting up your Okta application for multiple Amazon Q Business applications.

Making authenticated Amazon Q Business API calls using IAM federation

Amazon Q Business can securely handle data with integrated authentication and authorization. During data ingestion, Amazon Q Business preserves the authorization information—access control lists (ACLs)—from the data source so users can only request answers from the data they already have access to. Through IAM Federation, Amazon Q Business uses trusted identity propagation to ensure that an end user is authenticated and receives fine-grained authorization to their user ID and group-based resources.

In order to achieve this, a subset of the Amazon Q Business APIs (Chat, ChatSync, SearchRelevantContent, ListConversations, ListMessages, DeleteConversation, PutFeedback) require identity-aware AWS Sig V4 credentials for the authenticated user on whose behalf the API call is being made.

This page provides an overview of the workflows needed to obtain AWS Sig V4 credentials for a user authenticated using an identity provider (IdP), such as Okta. While we use Okta as an example, the same principles and steps apply to any other identity provider synced with your IAM instance.

Important

Amazon Q Business doesn't support OIDC for Google and Microsoft Entra ID.

Note

Federated groups aren't supported through IAM Federation. If you want to ingest federated groups, use the PutGroup API.

Topics

- Prerequisites
- One-time setup
- Workflow for each API call session for authenticated user

Prerequisites

Before you begin setting up for making Sig V4 authenticated API calls, make sure you've done the following:

- Created an Amazon Q Business application.
- Created an Okta IdP instance and configured users and groups within it. While we use Okta as an example, the same principles and steps apply to any other identity provider connected to your IAM instance.
- Created an IAM instance for your Amazon Q Business application and connected Okta as your identity source.
- Configured access to the AWS CLI.

One-time setup

The following section outlines the steps to set up the Amazon Q Business control plane. You only need to perform these steps once.

1. Create an OIDC app integration in Okta.

2. Create the IAM identity provider using the following command:

```
aws iam \
create-open-id-connect-provider \
--url issuer-url
```

   Then, copy the `OpenIDConnectProviderArn` from the output.

3. Next, create the IAM role. To do so, perform the following steps:

   a. Create a directory named `policies`.

   b. In that directory, create and save a file named `trustpolicyforfederation.json` with the following JSON included:

4. Next, create the IAM policy for your web experience. To do so, perform the following steps:

   - In the `policies` directory, create and save a new file named `permspolicyforfederation.json` with the following JSON included:

5. Finally, create and attach the roles in IAM using the following command:

```
aws iam \
create-role \
--role-name
--assume-role-policy-document file://policies/trustpolicyforfederation.json \
--policy-document file://policies/permspolicyforfederation.json
```

Workflow for each API call session for authenticated user

1. First, use the `IdToken` from Okta to call the AssumeRoleWithWebIdentity API to get AWS credentials. To do so, use the following command:

```
aws sts
assume-role-with-web-identity
--role-arn role arn
--role-session-name session-name
--web-identity-token id-token-from-okta
```

2. Then, set the following environment variables in your command line environment using the credentials you received as a response from the AssumeRoleWithWebIdentity API call.

```
AWS_ACCESS_KEY_ID="identity-aware-sigv4-access-key"
AWS_SECRET_ACCESS_KEY="identity-aware-sigv4-secret-key"
AWS_SESSION_TOKEN="identity-aware-sigv4-session-token"
```

3. Then, make Amazon Q Business API calls using the following command:

```
aws qbusiness \
chat-sync \
--application-id application-id
--user-message sample-chat-request
```

Managing Amazon Q Business resources

You can choose to manage your Amazon Q Business application environment and associated resources. To learn how to do so, see the following sections:

- Managing Amazon Q Business applications
- Managing Amazon Q Business web experiences
- Managing user subscriptions

Managing Amazon Q Business applications

To manage an Amazon Q Business application environment, you can take the following actions:

Actions

- Deleting an application
- Getting application environment properties
- Listing applications
- Updating an application environment

Deleting an application

To delete an Amazon Q Business application environment, you can use the console or the DeleteApplication API operation.

The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To delete an Amazon Q Business application

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, choose **Actions**.
3. Choose **Delete**.
4. In the dialog box that opens, type **`Delete`** to confirm deletion, and then choose **Delete**.

   You are returned to the service console while your application environment is deleted. When the deletion process is complete, the console displays a message confirming successful deletion.

AWS CLI

To delete an Amazon Q Business application environment

```
aws qbusiness delete-application \
--application-id application-id
```

Getting application environment properties

To get the properties of an Amazon Q Business application environment, you can use the console or the GetApplication API operation.

The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To get properties of an Amazon Q Business application environment

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. For **Applications**, select the name of your application environment from the list of applications.
3. On **Application settings**, the following properties are available:

- **Application name** – The name that you chose for your application environment.
- **Application ID** – The ID assigned to your application environment.
- **Subtitle** – The subtitle that you chose to assign to your application environment.
- **Service access** – The service access role that your application environment is using.
- **Title** – The title that you gave to your application environment.
- **Application status** – The status of your application environment.

To update a setting, select **Edit**.

AWS CLI

To get Amazon Q Business application properties

```
aws qbusiness get-application \
--application-id application-id
```

Listing applications

To list Amazon Q Business applications, you can use the console or the ListApplications API operation.

The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To list your Amazon Q Business application environments

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, all your configured application environments are listed.

AWS CLI

To list Amazon Q Business application environments

```
aws qbusiness list-applications \
```

```
--max-results max-results-to-return
```

Updating an application environment

To update an Amazon Q Business application environment, you can use the console or the UpdateApplication API operation.

> **Note**
>
> You can't update the retriever you've chosen or change users and groups added to the application environment when you update it. If you need to update your retriever, create a new application environment.
> If you're integrating your Amazon Q Business application environment with IAM Identity Center (IDC) as an AWS-managed application environment using and you want to update users and groups, you can do so from the application environment summary page.

The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To update an Amazon Q Business application environment

Option 1

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. In **Applications**, choose **Actions**.
4. Choose **Edit**.

   On the **Update application** page, edit your application environment settings.

Option 2

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.

3. On the application page, select **Edit** from the page header, or select **Edit** from **Application settings**.
4. Choose **Edit**.

   On the **Update application** page, edit your application environment settings.

AWS CLI

To update an Amazon Q Business application environment

```
aws qbusiness update-application \
--application-id application-id \
--display-name application-name \
--role-arn roleArn \
--description application-description \
--attachments-configuration attachmentsControlMode=ENABLED
```

Managing Amazon Q Business web experiences

To manage Amazon Q Business web experiences, you can take the following actions:

Actions

- Creating a web experience
- Deleting a web experience
- Getting properties of a web experience
- Listing web experiences
- Updating a web experience

Creating a web experience

To create an Amazon Q Business web experience, you can use the console or the CreateWebExperience API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

If you use the console, this action is spread across two steps: Creating an Amazon Q Business application using Identity Federation through IAM and Customizing web experience. To create a web experience, you must create an application environment.

AWS CLI

To create an Amazon Q Business web experience

```
aws qbusiness create-web-experience \
--application-id application-id \
--sample-prompts-control-mode sample-prompts \
--subtitle subtitle \
--tags tags \
--title title \
--welcome-message welcome-message \
```

Deleting a web experience

To delete an Amazon Q Business web experience, you can use the console or the DeleteWebExperience API operation.

If you're using the API, you can delete a web experience without deleting the application environment that it's a part of.

If you're using the console, the only way to delete your Amazon Q Business web experience is to delete the Amazon Q Business application environment that it's attached to.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To delete an Amazon Q Business web experience

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, choose **Actions**.
3. Choose **Delete**.

4. In the dialog box that opens, type **`Delete`** to confirm deletion, and then choose **Delete**.

   You are returned to the service console while your application environment is deleted. When the deletion process is complete, the console displays a message confirming successful deletion. Both the application environment and the web experience are deleted.

AWS CLI

To delete an Amazon Q Business web experience

```
aws qbusiness delete-web-experience \
--application-id application-id \
--web-experience-id web-experience-id
```

Getting properties of a web experience

To get the properties of an Amazon Q Business web experience, you can use the console or the GetWebExperience API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To get properties of an Amazon Q Business web experience

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. For **Web experience settings**, the following settings are available:

   - **Web experience IAM role ARN** – The IAM role assumed by end users when they log in to your web experience.
   - **Deployed URL** – The deployed URL of your web experience.
   - **Tags** – Tags that are attached to your web experience.

   To update a setting, choose **Edit**.

AWS CLI

To get properties of an Amazon Q Business web experience

```
aws qbusiness get-web-experience \
--application-id application-id \
--web-experience-id web-experience-id
```

Listing web experiences

To list Amazon Q Business web experiences, you can use the console or the ListWebExperiences API operation.

If you use the console, you can only see the web experience that's attached to a single application environment.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To list Amazon Q Business web experiences

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. For **Applications**, the Amazon Q Business web experience attached to your application environment is shown.

AWS CLI

To list Amazon Q Business web experiences

```
aws qbusiness get-web-experience \
--application-id application-id \
--web-experience-id web-experience-id \
--max-results max-results-to-return
```

Updating a web experience

To update an Amazon Q Business web experience, you can use the console or the UpdateWebExperience API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To update an Amazon Q Business web experience

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. Select **Customize web experience**.
4. Expand the right navigation menu to edit your web experience settings.

AWS CLI

To update an Amazon Q Business web experience

```
aws qbusiness update-web-experience \
--application-id application-id \
--web-experience-id web-experience-id \
--authentication-configuration authentication-configuration \
--sample-prompts-control-mode sample-prompts \
--subtitle subtitle \
--title title \
--welcome-message welcome-message
```

Managing subscriptions for applications using IAM Federation

To manage user subscriptions added to an application environment, you can perform the following actions:

Actions

- Updating subscription tiers
- Unsubscribing a user
- Listing user subscriptions

Updating subscription tiers

You can update a subscription tier using the AWS Management Console or the UpdateSubscription API operation.

Amazon Q Business automatically assigns subscriptions to users in an IAM-federated application. You can update the auto-subscription tier for your application. When you update the auto-subscription tier for the Amazon Q Business application, the new tier applies to new users logging into your web experience. Existing subscription types assigned to users don't get updated when you update your subscription tier.

You can also update the subscription tier for specific users already assigned subscriptions.

For more information on user subscriptions for an IAM federated Amazon Q Business application, see Subscriptions for applications using IAM Federation.

Console

To update auto-subscription tier for an Amazon Q Business application

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of the application environment that your uploaded files belong to.
3. From your applications page, select **Application settings**, and then select **Edit**.
4. From **Update application**, under **Default subscription settings**, in **Subscription tier**, choose between **Q Business Pro** and **Q Business Lite**.
5. Select **Update**.

To update a specific user's subscription

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of the application environment.

3. From your applications page, select **User access** and then select **Manage user access**.
4. On the **Manage access and subscriptions** page, from **Users**, select the user whose subscription you want to change and then select **Edit subscription**.
5. From the **Confirm subscription change** dialog box, from **New subscription**, and choose a new subscription tier.
6. Then, select **Confirm**.
7. On the **Manage access and subscriptions** page, select **Confirm** again.

AWS CLI

To update user or group subscriptions

```
aws qbusiness update-subscription \
--application-id application-id \
--subscription-id subscription-id \
--type subscription-type
```

Unsubscribing a user

When you remove a user, it cancels their subscription. The user continues to be visible in the list of users till the end of the month, after which they're removed from the list. An unsubscribed user can continue to use the application until the end of the month on their canceled subscription.

You can choose to re-activate and re-assign a subscription to an inactive user from the subscriptions list. When an unsubscribed user re-logs into a Amazon Q Business application, Amazon Q Business automatically re-assigns them a subscription based on the active subscription tier for your application. However, an unsubscribed user can continue to use the application until the end of the month of their canceled subscription. So, if they start re-using Amazon Q Business in the same month their subscription is canceled, they will keep the same subscription tier they were originally assigned during that month. You must cancel a subscription for a user removed from your identity provider to stop subscription charges for them.

If an unsubscribed user wants to maintain the subscription beyond the first month, and they start using Amazon Q Business again next month, then they will get assigned the default subscription tier of their application (which could be a different subscription tier than the one they were assigned originally).

Console

To unsubscribe a user from an Amazon Q Business application environment

1. From your Amazon Q Business application home page, scroll down to the **Users** section, select **Manage user access**.
2. On the **Manage subscriptions** page, from **Users**, select **Remove**.
3. From the **Unsubscribe and remove** box, choose **Done**.

AWS CLI

To cancel user or group subscriptions to Amazon Q Business

```
aws qbusiness cancel-subscription \
--application-id application-id \
--subscription-id subscription-id \
--type subscription-type
```

Listing user subscriptions

To see a list of user and group subscriptions within a specific Amazon Q Business application, you can use the AWS Management Console or the ListSubscriptions API operation.

For a consolidated view of your user subscriptions—including a list of subscribed users, their subscription status, and applications, accounts, or services a user can access through their subscriptions—you can also view the Amazon Q subscriptions page.

Console

To view a list of user and group subscriptions in an Amazon Q Business application environment

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of the application environment you created.
3. From your applications page, from the **User access** section, select **Manage user access**.
4. In the **Manage access and subscriptions** select **Users** if you want to view user subscriptions or **Groups** if you want to list group subscriptions.

To view a consolidated list of all user and group subscriptions across all Amazon Q Business application environments

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. Sign in to the AWS Management Console and open the Amazon Q Business console.
3. From the left navigation menu, choose **Subscriptions**,and then select **Users** if you want to view user subscriptions or **Groups** if you want to list group subscriptions.

AWS CLI

To list user or group subscriptions in an Amazon Q Business application

```
aws qbusiness list-subscriptions \
--application-id application-id
```

To list user or group subscriptions across all Amazon Q Business applications

This action is not supported.

Tagging resources in Amazon Q Business

Manage your Amazon Q Business applications and data sources by assigning tags. You can use tags to categorize your Amazon Q Business resources in various ways. For example, you could categorize by purpose, owner, or application, or any combination. Each tag consists of a *key* and a *value*, both of which you define.

Tags help you to do the following:

- **Identify and organize your AWS resources** – Many AWS services support tagging, so you can assign the same tag to resources in different services to indicate that the resources are related. For example, you can tag an Amazon Kendra retriever and the Amazon Q Business web experience that uses the retriever with the same tag.
- **Allocate costs** – You activate tags on the AWS Billing and Cost Management dashboard. AWS uses tags to categorize your costs and deliver a monthly cost allocation report to you. For more information, see Cost Allocation and Tagging in the *AWS Billing User Guide*.
- **Control access to your resources** – You can use tags in AWS Identity and Access Management (IAM) policies that control access to Amazon Q Business resources. To activate tag-based access

control, you can attach these policies to an IAM role or IAM user. For more information, see Authorization based on tags.

You can create and manage tags using the AWS Management Console, the AWS Command Line Interface (AWS CLI), or the Amazon Q Business API.

Topics

- Using tags
- Tag restrictions

Using tags

If you're using the console, you can tag resources when you create them or add them later. You can also use the console to update or remove tags in the following ways:

Adding tags

To add Amazon Q Business tags

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From **Applications**, select the application whose resources you want to tag.
3. From the application summary page, scroll down and select **Tags**.
4. In **Tags**, from the resource you want to add tags to, select **Manage tags**.
5. In **Tags – *optional***, select **Add new tag** to add tags to your Amazon Q Business resource. Then, enter the following information for each tag:
   - **Key** – Add a key for your tag.
   - **Value - *optional*** – An optional value for your tag.
6. Select **Save**.

Removing tags

To remove tags

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From **Applications**, select the application you want to delete tags from.

3. From the application summary page, scroll down and select **Tags**.
4. In **Tags**, from the resource you want to add tags to, select **Manage tags**.
5. In **Tags – *optional***, select **Remove**.
6. Select **Save**.

Listing tags

To view a list of tags

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From **Applications**, select the application you want to delete tags from.
3. From the application summary page, scroll down and select **Tags**.
4. In **Tags**, each tagged resource will display a list of tags associated with it.

If you're using the AWS CLI or the Amazon Q Business API, use the following operations to manage tags for your resources:

- CreateApplication – Apply tags when you create an Amazon Q Business application.
- CreateWebExperience – Apply tags when you create an Amazon Q Business web experience.
- ListTagsForResource – View the tags associated with a resource.
- TagResource – Add and modify tags for a resource.
- UntagResource – Remove tags from a resource.

Tag restrictions

The following restrictions apply to tags on Amazon Q Business resources:

- Maximum number of tags – 50
- Maximum key length – 128 characters
- Maximum value length – 256 characters
- Valid characters for key and value – a–z, A–Z, space, and the following characters: _ . : / = + - and @
- Keys and values are case sensitive
- Don't use `aws:` as a prefix for keys; it's reserved for AWS use

Creating an Amazon Q Business application environment for anonymous access

Amazon Q Business application environments support anonymous access, enabling unauthenticated user interactions with the Amazon Q generative AI assistant. You can also make selected enterprise data accessible to users without requiring credentials, such as website visitors seeking product information or support. This can be integrated through:

- Embedding the web experience URL in an iframe for quick deployment
- Using the `Chat`, `ChatSync`, and `PutFeedback` APIs to build custom interfaces

Billing for anonymous access application environments is based on usage. For more information, see Amazon Q Business pricing.

Important

Limitations of anonymous application environments

- You can create your anonymous application environment using Amazon Q Business Console, API, SDK, and AWS CLI. You can only use the application environment with the chat APIs. The following are the only chat APIs that support anonymous access application environments.
  - `Chat`
  - `ChatSync`
  - `PutFeedback`
- The web experience is only available for preview and testing purposes unless used within the context of an Amazon Q embedded implementation. For more information, see Amazon Q embedded.
- The GetDocumentContent API is not available for anonymous applications, consistent with other APIs such as GetMedia that require authentication.
- Chat history is not available for anonymous application environments
- Anonymous users and authenticated users are not supported on the same application environments

- Topic rules using users and groups are not supported for anonymous application environments
- Plugins are not supported for anonymous application environments
- Amazon Q Apps are not supported for anonymous application environments
- Attachments are not supported for anonymous application environments
- Admin controls and guardrails are read-only for anonymous application environments, except for blocked words.
- Amazon Q Business integrations are not supported for anonymous application environments
- The Amazon Q Quick integration is not supported for anonymous application environments
- You must only ingest publicly available data sources without access control lists (ACLs). Examples of public data sources include:
  - any data from the Amazon Q Business Web Crawler
  - S3 data without Amazon Q Business ACLs

All other Amazon Q Business functionality and features remain unchanged.

Topics

- Creating an a Amazon Q Business application environment for anonymous access
- Making authenticated Amazon Q Business API calls for application environment supporting anonymous access
- Managing resources for Amazon Q Business application environments that support anonymous access

Creating an a Amazon Q Business application environment for anonymous access

You can create an Amazon Q Business application environment that can be accessed anonymously using the Amazon Q Business Console, API, SDK, and AWS CLI. As a prerequisite, you must complete the setting up tasks. If you're using the AWS CLI or the API, you must create the required IAM roles.

The following tabs provide a procedure for creating your Amazon Q Business application environment with anonymous access using the Amazon Q Business console; and an example using the AWS CLI.

Console

To create an anonymous access application environment

1. Sign in to the Amazon Q Business console.
2. On the **Create application environment** page, for **What kind of application environment do you want to create?**, enter the following information for your Amazon Q Business application environment:

   a. **Application name** – A name for your Amazon Q Business application environment for easy identification. This name is only visible in the AWS Management Console. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters. Amazon Q Business auto-generates an application environment name for you, unless you choose to enter a custom name.

   b. **User Access** – Choose **Anonymous access**, users can then access this application environment without authentication.

   > **Note**
   >
   > The web experience is only available for preview and testing purposes *unless* used within the context of an Amazon Q embedded implementation. For more information, see Amazon Q embedded. If you want this capability, choose **Web experience**

3. For application environments with **Anonymous access**, you will be billed using usage based billing. For more information, see Amazon Q Business pricing.
4. For **Application details** – Amazon Q Business chooses the following configuration settings for your application environment by default:

   a. For **Application service access** – Amazon Q Business will create a new service-linked role for your application environment.

   b. **Encryption** – Amazon Q Business will create an AWS owned AWS KMS key to encrypt your data.

5. (Optional) To customize **Application details**, expand the **Application details section**, and then do the following:

    a. In **Application service access**, for **Choose a method to authorize Amazon Q Business**, choose from the following options:

        i. **Create and use a new service-linked role (SLR)** – Create and use a new Amazon Q Business-managed IAM role to allow it to access the AWS resources it needs to create your application environment.

        ii. **Create and use a new service role (SR)** – Create and use a new IAM role for Amazon Q Business to allow it to access the AWS resources it needs to create your application environment.

        iii. **Use an existing service role (SR)/service-linked role (SLR)** – Use an existing service role or service-linked IAM role to allow Amazon Q Business to access the AWS resources it needs to create your application environment.

        > **Note**
        >
        > For more information about example service roles, see IAM role for an Amazon Q Business application. For information on service-linked roles, including to manage them, see Using service-linked roles.

        iv. **Service role name** – A name for the service (IAM) role you created for easy identification on the console.

    b. For **Encryption** – Amazon Q Business encrypts your data by default using AWS managed AWS KMS keys. To customize your encryption settings, select **Customize encryption settings (advanced)**. Then, you can choose to use an existing AWS KMS key or create a new one.

6. For **Web experience service settings**, consider the following.

    a. **If you will use the web experience feature, choose a method to authorize Amazon Q Business** – A service access role assumed by your web experience that grants permission to have conversations anonymously. You can choose to use an existing role or create a new role.

    b. **Service role name** – A name for the service role you created for easy identification on the console.

7. To start creating your application environment, choose **Create**.

AWS CLI

To configure an Amazon Q Business application environment for anonymous access

```
aws qbusiness create-application \
--region your-region
--display-name application-name \
--identity-type ANONYMOUS \
--role-arn your-role-arn \
--description application-description \
--encryption-configuration kmsKeyId=<kms-key-id> \
```

> **Note**
>
> The web experience is only available for preview and testing purposes *unless* used within the context of an Amazon Q embedded implementation. For more information, see Amazon Q embedded.

To create an Amazon Q Business web experience

If you use the web experience, you must add the web experience permissions and trust IAM policies here.

```
aws qbusiness create-web-experience \
--application-id the-application-id-from-the-previous-step \
--role-arn iam-role-created \
--region your-region \
```

Making authenticated Amazon Q Business API calls for application environment supporting anonymous access

Amazon Q Business can securely handle data with integrated authentication and authorization. In order to achieve this, a subset of the Amazon Q Business APIs (Chat, ChatSync, and PutFeedback) require identity-unaware AWS Sig V4 credentials for the API call that is being made.

Topics

- Prerequisites
- One-time setup
- Workflow for each API call session

Prerequisites

Before you begin setting up for making Sig V4 authenticated API calls for anonymous application environments, make sure you've done the following:

- Created an Amazon Q Business anonymous application environment.
- Configured access to the AWS CLI.

One-time setup

The following section outlines the steps to set up the Amazon Q Business access for application environment that support anonymous access. You only need to perform these steps once.

1. Create a directory named *policies*.
2. Then, in the same directory, create and save a file named *permspolicyforAPIanonymous.json* with the following JSON.

   API permissions policy

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "QBusinessAnonymousConversationAPIPermissions",
            "Effect": "Allow",
            "Action": [
                "qbusiness:Chat",
                "qbusiness:ChatSync",
                "qbusiness:PutFeedback"
            ],
            "Resource": "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}"
        }]
}
```

3. Finally, create and attach the policy using the following commands in the AWS CLI.

Create and attach policy

```
aws iam \
create-role \
--role-name
--policy-document file://policies/permspolicyforAPIanonymous.json
```

Workflow for each API call session

1. First, call the AssumeRole API to get AWS credentials. To do so, use the following command:

   ```
   aws sts
   assume-role
   --role-arn role arn
   --role-session-name session-name
   ```

2. Then, set the following environment variables in your command line environment using the credentials you received as a response from the AssumeRole API call.

   ```
   AWS_ACCESS_KEY_ID="sigv4-access-key"
   AWS_SECRET_ACCESS_KEY="sigv4-secret-key"
   AWS_SESSION_TOKEN="sigv4-session-token"
   ```

   Then, make Amazon Q Business API calls using the following command:

   ```
   aws qbusiness \
   chat-sync \
   --application-id application-id
   --user-message sample-chat-request
   ```

Managing resources for Amazon Q Business application environments that support anonymous access

You can choose to manage your Amazon Q Business application environment and associated resources. To learn how to do so, see the following sections:

Topics

- Example IAM policies for Amazon Q Business application environment supporting anonymous access
- Managing Amazon Q Business anonymous application environments
- Managing Amazon Q Business web experiences for anonymous access

Example IAM policies for Amazon Q Business application environment supporting anonymous access

We strongly recommend that you use a restricted policies for the role that will be used to call the chat APIs for anonymous access application environments.

You need permission policies to use Amazon Q Business application environments that support anonymous access. The following are examples of such restricted policies.

Topics

- Policy for calling relevant APIs
- Policies for using the web experience

Policy for calling relevant APIs

Example policy to allow the Amazon Q Business APIs for anonymous access

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "QBusinessAnonymousConversationAPIPermissions",
            "Effect": "Allow",
            "Action": [
                "qbusiness:Chat",
                "qbusiness:ChatSync",
                "qbusiness:PutFeedback"
            ],
            "Resource": "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}"
        }]
}
```

Applying your restricted policies to an IAM role for using APIs for Amazon Q application environments supporting anonymous access

1. Create a directory named *policies*.
2. In that directory, create and save a file named *permspolicyforAPIanonymous.json* with the JSON for allowing Amazon Q Business API calls for anonymous access.
3. Finally, create and attach the policy using the following commands in the AWS CLI.

   Create and attach policy

   ```
   aws iam \
   create-role \
   --policy-document file://policies/permspolicyforAPIanonymous.json
   ```

Policies for using the web experience

Example policy to allow the Amazon Q Business web experience for anonymous access

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "QBusinessAnonymousWebExperienceConversationPermissions",
            "Effect": "Allow",
            "Action": [
                "qbusiness:Chat",
                "qbusiness:ChatSync",
                "qbusiness:PutFeedback",
                "qbusiness:GetChatControlsConfiguration",
                "qbusiness:GetApplication",
            ],
            "Resource": "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}"
        }]
}
```

Example trust policy to allow the Amazon Q Business web experience for anonymous access

```
{
    "Version": "2012-10-17",       ,
    "Statement": [
```

```
        {
            "Sid": "QBusinessTrustPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "application.qbusiness.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{{account_id}}"
                },
                "ArnEquals": {
                    "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{account_id}}:application/{{application_id}}"
                }
            }
        }
    ]
}
```

Applying your restricted policies for using the web experience to an IAM role

1. Create a directory named *policies*.
2. Then, in the same directory, create and save a file named *permspolicyforwebexperienceanonymous* with the JSON for allowing the Amazon Q Business web experience for anonymous access.
3. Then, in the same directory, create and save a file named *trustpolicyforanonymous.json* with the JSON for the trust policy to allow the Amazon Q Business web experience for anonymous access
4. Finally, create and attach the policies using the following commands in the AWS CLI.

   Create and attach policy

   ```
   aws iam \
   create-role \
   --role-name --assume-role-policy-document file://policies/
   trustpolicyforanonymous.json \
   ```

```
--policy-document file://policies/permspolicyforwebexperienceanonymous.json
```

> **Note**
>
> For the web experience to work properly with AWS CLI commands both policies are needed

Amazon Q also supports using a service-linked role (`AWSServiceRoleForQBusiness`) for an Amazon Q application environment. The following is the service-linked role policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessPutMetricDataPermission",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/QBusiness"
                }
            }
        },
        {
            "Sid": "QBusinessCreateLogGroupPermission",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/qbusiness/*"
            ]
        },
        {
            "Sid": "QBusinessDescribeLogGroupsPermission",
```

```
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "QBusinessLogStreamPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogStreams",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/qbusiness/*:log-stream:*"
            ]
        }
    ]
}
```

For more information on using service-linked roles for an Amazon Q application environment, see Using service-linked roles.

Managing Amazon Q Business anonymous application environments

To manage an Amazon Q Business application environment, you can take the following actions:

Actions

- Deleting an anonymous application environment
- Getting anonymous application environment properties
- Listing anonymous application environments
- Updating an application environment

Deleting an anonymous application environment

To delete an Amazon Q Business anonymous application environment, you can use the console or the DeleteApplication API operation.

The following tabs provide a procedure for the console and code example for the AWS CLI.

Console

To delete an Amazon Q Business application environment

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, choose **Actions**.
3. Choose **Delete**.
4. In the dialog box that opens, type **`Delete`** to confirm deletion, and then choose **Delete**.

   You are returned to the service console while your application environment is deleted. When the deletion process is complete, the console displays a message confirming successful deletion.

AWS CLI

To delete an Amazon Q Business application environment

```
aws qbusiness delete-application \
--application-id application-id
```

Getting anonymous application environment properties

To get the properties of an Amazon Q Business application environment, you can use the console or the GetApplication API operation.

The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To get properties of an Amazon Q Business application environment

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. For **Applications**, select the name of your application environment from the list of application environments.
3. On **Application settings**, the following properties are available:

   - **Application name** – The name that you chose for your application environment.

- **Application ID** – The ID assigned to your application environment.
- **Subtitle** – The subtitle that you chose to assign to your application environment.
- **Service access** – The service access role that your application environment is using.
- **Title** – The title that you gave to your application environment.
- **Application status** – The status of your application environment.

To update a setting, select **Edit**.

AWS CLI

To get Amazon Q Business application environment properties

```
aws qbusiness get-application \
--application-id application-id
```

Listing anonymous application environments

To list Amazon Q Business application environments, you can use the console or the ListApplications API operation.

The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To list your Amazon Q Business application environments

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, all your configured application environments are listed.

AWS CLI

To list Amazon Q Business application environments

```
aws qbusiness list-applications \
--max-results max-results-to-return
```

Updating an application environment

To update an Amazon Q Business application environment, you can use the console or the UpdateApplication API operation.

The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To update an Amazon Q Business application environment

Option 1

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of application environments.
3. In **Applications**, choose **Actions**.
4. Choose **Edit**.

   On the **Update application environment** page, edit your application environment settings.

Option 2

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of application environments.
3. On the application environment page, select **Edit** from the page header, or select **Edit** from **Application settings**.
4. Choose **Edit**.

   On the **Update application environment** page, edit your application environment settings.

AWS CLI

To update an Amazon Q Business application environment

```
aws qbusiness update-application \
--application-id application-id \
```

```
--display-name application-name \
--role-arn your-role-arn \
--description application-description \
```

Managing Amazon Q Business web experiences for anonymous access

To manage Amazon Q Business web experiences for anonymous access, you can take the following actions:

Actions

- Share an anonymous web experience
- Deleting a web experience
- Getting properties of a web experience
- Listing web experiences
- Updating a web experience

Share an anonymous web experience

If you created a web experience when you created your application, you can preview that Amazon Q Business web experience for anonymous access, using the console or the CreateAnonymousWebExperienceUrl API operation.

Note

- The preview URL for the web experience is for one-time use only and has to be regenerated every time. This URL must be accessed within 5 minutes of creation. Once accessed, the session remains active for the configured duration. To use the web experience in your applications, you must use the Amazon Q embedded feature and call the CreateAnonymousWebExperienceUrl API operation whenever you need a new application session or after one hour whichever comes first.
- All anonymous web experience URLs generated are able to process billable chat requests until the sessions expire. For more information, see Amazon Q Business pricing.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

1. After Creating an anonymous access application environment in the console with a web experience, you can navigate to your anonymous application.
2. In the **Web experience settings** section in the console, you can **Preview web experience** to view the web experience.
3. Alternatively, you can choose to **Share the web experience URL** to share the web experience. To do this, you can choose the duration your **Testing link is valid for** and choose **Create URL**. The URL will be automatically copied to your clipboard.

AWS CLI

To share an Amazon Q Business anonymous web experience url

After Creating an anonymous access application environment with a web experience, you can do the following.

```
aws qbusiness create-anonymous-web-experience-url \
--application-id <your-application-id> \
--web-experience-id <web-experience-id>
--session-duration-in-minutes<x-minutes >
```

Deleting a web experience

To delete an Amazon Q Business web experience, you can use the console or the DeleteWebExperience API operation.

If you're using the API, you can delete a web experience without deleting the application environment that it's a part of.

If you're using the console, the only way to delete your Amazon Q Business web experience is to delete the Amazon Q Business application environment that it's attached to.

> **Note**
>
> Even after deleting the web experience all URLs connected to this web experience continue to process billable chat requests until their sessions expire. For more information, see Share an anonymous web experience.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To delete an Amazon Q Business web experience

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, choose **Actions**.
3. Choose **Delete**.
4. In the dialog box that opens, type **`Delete`** to confirm deletion, and then choose **Delete**.

   You are returned to the service console while your application environment is deleted. When the deletion process is complete, the console displays a message confirming successful deletion. Both the application environment and the web experience are deleted.

AWS CLI

To delete an Amazon Q Business web experience

```
aws qbusiness delete-web-experience \
--application-id application-id \
--web-experience-id web-experience-id
```

Getting properties of a web experience

To get the properties of an Amazon Q Business web experience, you can use the console or the GetWebExperience API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To get properties of an Amazon Q Business web experience

1. Sign in to the AWS Management Console and open the Amazon Q Business console.

2. In **Applications**, select the name of your application environment from the list of applications.
3. For **Web experience settings**, the following settings are available:

   - **Web experience IAM role ARN** – The IAM role assumed by end users when they log in to your web experience.
   - **Deployed URL** – The deployed URL of your web experience.
   - **Tags** – Tags that are attached to your web experience.

   To update a setting, choose **Edit**.

AWS CLI

To get properties of an Amazon Q Business web experience

```
aws qbusiness get-web-experience \
--application-id application-id \
--web-experience-id web-experience-id
```

Listing web experiences

To list Amazon Q Business web experiences, you can use the console or the ListWebExperiences API operation.

If you use the console, you can only see the web experience that's attached to a single application environment.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To list Amazon Q Business web experiences

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. For **Applications**, the Amazon Q Business web experience attached to your application environment is shown.

AWS CLI

To list Amazon Q Business web experiences

```
aws qbusiness get-web-experience \
--application-id application-id \
--web-experience-id web-experience-id \
--max-results max-results-to-return
```

Updating a web experience

To update an Amazon Q Business web experience, you can use the console or the UpdateWebExperience API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To update an Amazon Q Business web experience

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. Select **Customize web experience**.
4. Expand the right navigation menu to edit your web experience settings.

AWS CLI

To update an Amazon Q Business web experience

```
aws qbusiness update-web-experience \
--application-id application-id \
--web-experience-id web-experience-id \
--subtitle subtitle \
--title title \
--welcome-message welcome-message
```

Creating an Amazon Quick-integrated Amazon Q Business application

With an Amazon Quick-integrated Amazon Q Business application, Quick users authenticate through Amazon Quick and access answers from unstructured data in Amazon Q Business. Amazon Quick is a business intelligence service that provides insights from your structured data, such as databases, data lakes, and data warehouses.

With Quick authentication, your Amazon Quick administrator uses Quick as a single point of entry to manage access to unstructured data in Amazon Q Business. You can manage users and groups without reliance on AWS IAM Identity Center, including permissions, governance, and access controls.

After you set up Quick as your authentication, users sign in through Quick with their existing credentials. After authentication, they can use Quick Q&A and Data Stories to get answers to questions based on your unstructured enterprise data in Amazon Q Business and your structured data analytics.

You can create an Quick integrated Amazon Q Business application environment from Amazon Quick or you can create it with the Amazon Q Business CreateApplication API operation.

Topics

- Considerations
- Creating a Quick-integrated application from Amazon Quick
- Creating a Quick-integrated application with Amazon Q Business API operations

Considerations

The following limitations apply to the Amazon Q application.

- Quick and Amazon Q Business must exist in the same AWS account. Cross account calls are not supported.
- Quick and Amazon Q Business accounts must exist in the same AWS Region. Cross-region calls are not supported. For a list of all supported Quick Regions, see Supported AWS Regions for Amazon Q in QuickSight. For a list of all supported Amazon Q Business Regions, see Service quotas for Amazon Q Business.

If your Quick account exists in more than one region, you can connect one Amazon Q Business application from each region to the Quick account. For example, if your Quick account exists in US East (N. Virginia) and US West (Oregon), one Amazon Q Business application located in US East (N. Virginia) and one Amazon Q Business application located in US West (Oregon) can be connected to the Quick account.

- Quick and Amazon Q Business accounts that are integrated need to use the same identity methods. For example, if a Quick account uses IAM Identity Center for identity management, the Amazon Q Business account that it is integrating with must also use IAM Identity Center for identity management.
- Email addresses that are associated with Quick users and groups are used to perform authorization checks in Amazon Q Business.
- To create an Amazon Q Business application with the CreateApplication API operation, the user or role must have permissions to create an application. For more information about setting up Amazon Q Business, see Setting up for Amazon Q Business.

Creating a Quick-integrated application from Amazon Quick

To set up an Quick-integrated Amazon Q Business application environment, Quick administrators can create a new application from the Quick admin portal or connect to an existing one. After you create an application environment, you create an index and add a data source in Amazon Q Business.

- For information on setting up and managing a Quick-integrated Amazon Q Business application from Quick, see Augmenting Amazon QuickSight generative BI capabilities with Amazon Q in the *Amazon Quick User Guide*.
- For information about adding a data source to an Amazon Q application, see Connecting Amazon Q Business data sources.

Creating a Quick-integrated application with Amazon Q Business API operations

To create an Amazon Quick integrated application environment with Amazon Q Business APIs, you use the CreateApplication API operation. For `identityType`, specify `AWS_QUICKSIGHT_IDP`. In `QuickSightConfiguration`, specify the `clientNamespace`. This is the Quick namespace that

you use as your identity provider. For more information about Quick namespaces, see Namespace operations.

The following example shows how to use the AWS Command Line Interface (AWS CLI) to create a Quick-integrated application environment.

```
aws qbusiness create-application \
--display-name MyQBusinessApp \
--identity-type AWS_QUICKSIGHT_IDP \
--quick-sight-configuration '{"clientNamespace": "my-quicksight-namespace"}'
```

Enhancing an Amazon Q Business application environment

After you finish configuring your application environment, you can optionally choose to enhance it.

You can choose from the following available enhancements:

- **Data sources** – Connect data sources to your application environment.
- **Admin controls and guardrails** – Customize blocked topics and choose the knowledge sources your web experience uses for responses.
- **Response customization** – Configure how Amazon Q Business generates and formats responses to user queries, including style, tone, and length.
- **Amazon Q Apps** – Create lightweight, purpose-built apps within your broader Amazon Q Business application environment. Using enterprise data, users can create a generative AI-powered app that streamlines their tasks.
- **Plugins** – Enable your end users to perform specific tasks related to third-party services from within their web experience chat—like creating Jira tickets.
- **Document enrichment** – Control document attribute ingestion and build customized data solutions.
- **Metadata boosting** – Use document attributes to boost response generation from specific content within your application environment.
- **Metadata controls** – Enable document attributes for end user search.

Topics

- Connecting Amazon Q Business data sources
- Admin controls and guardrails in Amazon Q Business
- Customizing responses in Amazon Q Business
- Share your enterprise data with data accessors using Amazon Q index
- Amazon Q embedded
- Integrations
- Creating purpose-built Amazon Q Apps
- Document enrichment in Amazon Q Business

- Extracting semantic meaning from embedded visual content with Amazon Q Business
- Tuning the query results based on document attribute relevancy
- Boosting chat responses using metadata boosting
- Configuring metadata controls in Amazon Q Business

Connecting Amazon Q Business data sources

A *data source* allows you to combine data from different places into one central index for your Amazon Q Business application. Amazon Q Business provides several easy ways to connect your data.

Before adding any data, you need to set up a retriever and an index for your application. Once that's done, you can add data in three ways:

- **Upload documents directly** – Upload documents directly using the console or using the BatchPutDocument API operation.
- **Connecting a Amazon Q Business data source** – Use the AWS Management Console or the the CreateDataSource API operation to connect a supported data source connector to your Amazon Q Business application.

  > **Note**
  >
  > You must create an Amazon Q Business index to store your data before you connect a data source to your application.

- **Connecting Amazon Kendra data sources** – Use existing Amazon Kendra data sources by connecting a Amazon Kendra index as a retriever.

  If you're connecting a Amazon Kendra GenAI Enterprise Edition index from an Amazon Q Business application, you can detach it and use it with other AWS Gen AI services, like Amazon Bedrock. Detaching an Amazon Kendra index automatically deletes the retriever Amazon Q Business created for it. For a list of features supported by Amazon Kendra GenAI Enterprise indices, see Amazon Kendra GenAI Enterprise Edition index.

> **Note**
>
> Amazon Q Business uses user email ID to determine end user access to documents in an index. When you connect an Amazon Kendra index to Amazon Q Business, Amazon Q Business relays the user's identifying email ID to Amazon Kendra to enable document filtering for end users. If data sources connected to your Amazon Kendra index don't use email-ID based document filtering, or the email ID is not present, Amazon Q Business generates responses only from public documents.

Topics

- Creating an index for an Amazon Q Business application
- Uploading files
- Connecting Amazon Q Business data source connectors
- Troubleshooting data source connectors
- Managing Amazon Q Business data source resources

Creating an index for an Amazon Q Business application

Before you can add data in your Amazon Q Business application, you need to connect it to the following components:

- An **index** – This is where the data you add is stored and organized.
- A **retriever** – This is the tool that fetches data from an index during conversations.

Once these are created, you can then add data sources and configure features like metadata boosting or document enrichment.

You have two options for indices and retrievers to connect to your application:

- **Amazon Q Business native index and retriever** – Amazon Q Business provides a native index you can add your data to. Choosing this index creates an Amazon Q Business index that can connect to the Amazon Q Business supported data sources that you choose.
- **Amazon Kendra index and retriever** – If you're already an Amazon Kendra customer, you can connect your Amazon Kendra index with data sources attached to your Amazon Q Business

application and use it as a retriever. You create an Amazon Kendra index using the Amazon Kendra console or API, and add it as a retriever when using the Amazon Q Business console or API.

> **Note**
>
> The option to create an Amazon Kendra index is visible on the console only if you're already an Amazon Kendra user.
> If you're connecting a Amazon Kendra GenAI Enterprise Edition index from an Amazon Q Business application, you can detach it and use it with other AWS Gen AI services, like Amazon Bedrock. Detaching an Amazon Kendra index automatically deletes the retriever Amazon Q Business created for it. For a list of features supported by Amazon Kendra GenAI Enterprise indices, see Amazon Kendra GenAI Enterprise Edition index.

> **Note**
>
> Amazon Q Business uses user email ID to determine end user access to documents in an index. When you connect an Amazon Kendra index to Amazon Q Business, Amazon Q Business relays the user's identifying email ID to Amazon Kendra to enable document filtering for end users. If data sources connected to your Amazon Kendra index don't use email-ID based document filtering, or the email ID is not present, Amazon Q Business generates responses only from public documents.

For instructions on how to select an index and retriever, choose a topic based on your index preference for Amazon Q.

Topics

- Creating an Amazon Q Business index
- Connecting an Amazon Kendra index as retriever

Creating an Amazon Q Business index

To create a Amazon Q Business index and retriever, you can use either the AWS Management Console, or the CreateIndex and CreateRetriever API operations.

If you use the AWS Management Console, Amazon Q Business creates a retriever for you when you create the index. When you use the API, you need to create a retriever for your index separately.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To create an Amazon Q Business retriever

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. Complete the steps to create your Amazon Q Business application.
3. In **Applications**, select the name of your application from the list of applications.
4. From the left navigation menu, choose **Data sources**.
5. From the **Data sources** page, choose **Add index**.
6. From the **Add index** page, choose **Create a new index** and then do the following:

    a. In **Name your index with a unique identifier**, for **Index name**, input a name for your Amazon Q Business application.

    You can include hyphens (-), but not spaces. Maximum of 1000 alphanumeric characters.

    > **Important**
    >
    > You can't change the name of the index after it's created.

    > **Note**
    >
    > Available data sources when you select this option include all Amazon Q Business supported data connectors and direct document upload.

    b. In **Index provisioning**, do the following:

    i. Choose between **Enterprise** and **Starter** index types based on your use case. For more information on index types, see Index types.

ii. For **Number of units** – Choose the number of index units that you need. Amazon Q Business charges you based on the document capacity that you choose. If you choose an Enterprise index, You can choose up to 50 units. If you choose a Starter index, you can choose up to 5 units. Each unit is 20,000 documents or 200 MB, whichever is reached first. For more information on index provisioning pricing, see Amazon Q Business pricing.

7. To create your index and retriever, choose **Add index**.

AWS CLI

To create an Amazon Q Business index

```
aws qbusiness create-index \
--application-id application-id \
--display-name display-name \
--description index-description \
--capacity-configuration units =<index-capacity-units> \
--type ENTERPRISE | STARTER
```

To create an Amazon Q Business retriever

```
aws qbusiness create-retriever \
--application-id application-id \
--display-name display-name \
--type NATIVE_INDEX \
--role-arn roleArn \
--configuration nativeIndexConfiguration="{indexId=<created-index-id>}" \
--tags tags
```

Connecting an Amazon Kendra index as retriever

If you use Amazon Kendra, you can connect an existing Amazon Kendra index as a retriever to your Amazon Q Business application environment.

You create a Amazon Kendra index using the Amazon Kendra console and API. To connect a Amazon Kendra index to Amazon Q Business, you can use the Amazon Q Business console or the CreateRetriever API operation.

If you're connecting a Amazon Kendra GenAI Enterprise Edition index from an Amazon Q Business application, you can detach it and use it with other AWS Gen AI services, like Amazon Bedrock. Detaching an Amazon Kendra index automatically deletes the retriever Amazon Q Business created for it. For a list of features supported by Amazon Kendra GenAI Enterprise indices, see Amazon Kendra GenAI Enterprise Edition index.

Note

If you choose to use an Amazon Kendra index as retriever, data in your Amazon Kendra will be connected to your Amazon Q Business application environment. If you use an Amazon Kendra index, you can't use Amazon Q Business data connectors or direct document upload for your application environment.

Note

Amazon Q Business uses user email ID to determine end user access to documents in an index. When you connect an Amazon Kendra index to Amazon Q Business, Amazon Q Business relays the user's identifying email ID to Amazon Kendra to enable document filtering for end users. If data sources connected to your Amazon Kendra index don't use email-ID based document filtering, or the email ID is not present, Amazon Q Business generates responses only from public documents.

For more information about Amazon Kendra, see the following topics in the Amazon Kendra User Guide and API Reference:

- What is Amazon Kendra?
- Creating a data source connector
- Amazon Kendra API Reference

The following tabs provide a procedure for the AWS Management Console and code samples for the AWS CLI.

Console

To connect an Amazon Kendra index

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. Complete the steps to create your Amazon Q Business application.
3. In **Applications**, select the name of your application from the list of applications.
4. From the left navigation menu, choose **Data sources**.
5. From the **Data sources** page, choose **Add index**.
6. From the **Add index** page, choose **Use an existing Amazon Kendra index** and then do the following:

    a. In **Select an index**, select an existing Amazon Kendra index. All data sources synced to your Amazon Kendra index will be connected to your Amazon Q Business application environment.

    b. For **Authorization** – Create and use a new service role to connect Amazon Kendra to Amazon Q Business or use an existing one.

    c. For **Service role name** – Provide a name for your IAM access role. Or, choose to use the auto-generated role that's provided.
7. Select **Add index**, to connect your Amazon Kendra index to your application.

AWS CLI

To connect an Amazon Kendra index

```
aws qbusiness create-retriever \
--display-name display-name \
--type KENDRA_INDEX \
--role-arn roleArn \
--configuration kendraIndexConfiguration="{indexId=<kendra-index-id>
```

Uploading files

To upload documents directly to an Amazon Q Business application environment, you can use the AWS Management Console or the BatchPutDocument API operation.

If you use an Amazon Kendra index to retrieve your documents, you can't directly upload documents.

> **Note**
>
> This procedure is available if you chose to create a new Amazon Q Business index for your application environment. Files can only be uploaded after the Amazon Q Business index and retriever creation process has completed.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To upload files

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. Complete the steps to create your Amazon Q Business application.
3. Complete the steps for creating an Amazon Q Business index.
4. Then, from the left navigation menu, choose **Data sources**.
5. From the **Data sources** page, choose **Add data source**.
6. Then, on the **Add data sources** page, from **Data sources** choose **Upload files**.
7. Then, in **Upload files**, select one of the following methods to add your files:
   - Drag and drop the document files that you want to upload.
   - Add your documents to the application environment, and then select **Choose files**.
8. After choosing your files, choose **Upload**.

   You are returned to the Amazon Q Business console while your documents are uploaded. The console displays a confirmation message when your documents are successfully uploaded.

AWS CLI

To upload documents directly

```
aws qbusiness batch-put-document \
--application-id application-id \
```

```
--index-id index-id \
--documents documents-to-add \
--data-source-sync-id data-source-sync-id \
--role-arn roleArn
```

Connecting Amazon Q Business data source connectors

> **Note**
>
> Before you connect an Amazon Q Business data source to your application, you must add an index and retriever to it.

To connect a data source to your Amazon Q Business application environment, you can use the AWS Management Console or the CreateDataSource API operation.

By using the `CreateDataSource` API operation, you can configure tags, sync run schedules, and configure Amazon VPC settings. Then, you can use the `configuration` parameter to provide all other configuration information specific to your data source connector.

> **Note**
>
> This procedure is available if you chose to add a new Amazon Q Business index to your application environment.

This section contains an overview of data source connector features, recommended best practices for configuration, and configuration information specific to your data source connector.

Topics

- Data source connector concepts
- What is a document?
- Best practices for data source connector configuration in Amazon Q Business
- Supported connectors
- Understanding Amazon Q Business User Store
- Using Amazon VPC with Amazon Q Business connectors

Data source connector concepts

This topic outlines specific concepts and features of Amazon Q Business data source connectors. These concepts are key to understanding how to configure your connector setup. These terms recur on the AWS Management Console, AWS Command Line Interface (AWS CLI), and the Amazon Q API.

Topics

- Source and endpoint metadata
- Authorization
- Authentication
- Virtual private cloud
- Web proxy
- IAM role
- Identity crawler
- Sync scope
- Sync mode
- Sync run schedule
- Field mappings

Source and endpoint metadata

You enter your data source configuration information in the **Source** section on the console. If you use the API, you specify this information using the `configuration` parameter of the `CreateDataSource` operation. Connection configuration information varies depending on the data source. To make sure your connector configures correctly, check the following details:

- You're following connector configuration best practices.
- You've completed the prerequisites for data source configuration. Prerequisites information specific to your data source connector is on each connector's specific page.

Authorization

Amazon Q Business connectors index access control list (ACL) information that's attached to a document along with the document itself. For document access control lists, Amazon Q Business indexes the following:

- user email address
- group name for the local group
- group name for the federated group (for example, if you have a Microsoft SharePoint data source integrated with Microsoft Entra ID (formerly Azure AD)

Then, Amazon Q Business stores the ACL information it indexes in the Amazon Q Business User Store to create user and group mappings and filter chat responses based on the end user's access to documents.

An Amazon Q Business connector updates any changes in ACLs each time that your data source content is crawled. To capture ACL changes to make sure that the right end users have access to the right content, re-sync your data source regularly.

Connectors support crawling ACL and identity information for all data sources where the feature is supported. To index documents without ACLs (as public documents) ensure these documents are already marked public in the enterprise data source the connectors index the content from.

> **Note**
>
> Amazon Q Business supports crawling ACLs for document security by default. As a general rule, turning off ACLs and identity crawling once they have been enabled are no longer supported. In preparation for connecting Amazon Q Business applications to IAM Identity Center, enable ACL indexing and identity crawling for secure querying and re-sync your connector. Once you turn ACL and identity crawling on you won't be able to turn them off. Certain connectors provide you with the ability to manage ACLs by enabling or disabling them during data source creation. To create a data source with ACLs disabled, you need specific IAM permissions. For more information, see Setting up.

If you delete a group in the User Store and then re-create it later with the same name but with different group members, document ACLs which contain this group may be impacted. We

recommend that this type of change (deleting or re-creating a group with the same name but with different group members) be done in the data source instead of the Amazon Q Business User Store.

If you re-use an email address between users (for example a user leaves the company and at a later time a new user joins the company and has the same email address), you must delete the original user from the User Store. Amazon Q Business will verify if all the attributes of the new user from the IAM Identity Center matches those of the user in the User Store. If an older user with the same email address but with different attributes is found, the API calls for that user (for example, the query request) will be denied.

Important

Inadvertent mistakes when you update the User Store's user, group, group membership, and mapping information can result in unintentional and unacceptable changes in the accessibility of documents to users.
Treat the ability to update the User Store to create users, update users, delete users, create groups, update groups, delete groups (i.e, create update delete operations), and update the mappings, as a privileged operation.
Ensure that access to the User Store APIs is provided only to admin who fully understand how to use these APIs and the implications of these changes on your document security.
We recommend establishing a documented approval process be followed for making such changes.

Authentication

To authenticate Amazon Q Business to access your data source, you provide your data source access credentials to Amazon Q Business using an AWS Secrets Manager secret. If you use the console, you can choose to create a new secret or use an existing one. If you use the API, you must provide the Amazon Resource Name (ARN) of an existing Secrets Manager secret when you use the `CreateDataSource` operation.

Note

You should regularly refresh or rotate your credentials and secret details. Provide only the necessary access level for your own security. Don't re-use credentials and secrets across data sources.

For on-premises or server data source connectors, Amazon Q Business checks if the endpoint information included in Secrets Manager is the same endpoint information specified in your data source configuration details. This helps protect against the confused deputy problem, which is a security issue. The problem occurs when a user doesn't have permissions to perform an action. But, by using Amazon Q Business as a proxy, the user can access the configured secret and perform the action.

If you change your endpoint information later, you must create a new secret to sync this information.

> **Note**
>
> If you change your authentication type and credentials, you must update your IAM role to access the correct Secrets Manager secret ID.

Virtual private cloud

Amazon Q Business can connect to Amazon Virtual Private Cloud to index content stored in data sources or databases running in your private cloud. If your data source or database isn't running on Amazon VPC, you can connect your data source or database to Amazon VPC using a virtual private network (VPN).

You can use Amazon VPC with either the console or the Amazon Q Business API. If you're using the API, you specify the `vpcConfiguration` when you use the `CreateDataSource` API operation.

If you're using Amazon VPC with Amazon Q Business, you need the following information:

- The identifier of the subnet that contains the data source.
- The identifier of the security groups that grant access to the host.
- An IAM role with access to Amazon VPC and permissions to create and delete an elastic network interface in your subnets is also required.

You can find the subnet and security group IDs in the Amazon VPC console. For more information, see What is Amazon VPC? in the *Amazon VPC User Guide*.

For more information about using Amazon VPC with Amazon Q Business, see Using Amazon VPC with connectors..

Web proxy

For all supported data sources, you can use a web proxy to connect to your data source instance. You must provide the host name and port number. For example, `a.example.com` is the hostname of `https://a.example.com/page1.html`, and the port is 443, which is the standard port for HTTPS.

> **Important**
>
> For security reasons, Amazon Q Business only supports web proxy using HTTPS protocol.

IAM role

To create your data source connector, Amazon Q Business requires permissions to interact with other services.

If you're using the console, you can choose an existing IAM role or let Amazon Q Business create a role for you. If you're unsure if an existing role is used for an application, choose **Create a new role** to avoid an error.

> **Note**
>
> To **Create a new role** during connector configuration on the console, you must have permissions to create an IAM role.

If you're using the API, you must provide the ARN of an existing IAM role when you use the `CreateDataSource` operation.

IAM roles used for applications can't be used for data sources.

> **Note**
>
> Make sure your IAM role includes the permissions to support your Amazon Q Business connector configurations.

Identity crawler

Amazon Q Business crawls ACL information at the document level from supported data sources. In addition, Amazon Q Business crawls and stores principal information within each data source (local user alias, local group, and federated group identity configurations) into the Amazon Q Business User Store. This is useful when your application environment is connected to multiple data sources with different authorization and authentication systems, but you want to create a unified, access-controlled chat experience for your end users.

Amazon Q Business indexes the following information from document access control lists:

- user email address
- group name for the local group
- group name for the federated group (for example, if you have a Microsoft SharePoint data source integrated with Microsoft Entra ID (formerly Azure AD)

Amazon Q Business internally maps the local user and group IDs attached to the document to the federated identities of users and groups. Mapping identities streamlines user management and speeds up chat responses by reducing ACL information retrieval time during chat requests. Identity crawling, along with the Authorization feature, helps to filter and generate web experience content restricted by end user context. For more information about this process, Amazon Q Business User Store.

Connectors support crawl ACL and identity information where applicable based on the data source. To index documents without ACLs (as public documents) ensure the documents you want to index from your data source are public documents in the enterprise data source the connectors index the content from.

If you delete a group in the User Store and then re-create it later with the same name but with different group members, document ACLs which contain this group may be impacted. We recommend that this type of change (deleting or re-creating a group with the same name but with different group members) be done in the data source instead of the Amazon Q Business User Store.

If you re-use an email address between users (for example a user leaves the company and at a later time a new user joins the company and has the same email address), you must delete the original user from the User Store. Amazon Q Business will verify if all the attributes of the new user from the IAM Identity Center matches those of the user in the User Store. If an older user with the same

email address but with different attributes is found, the API calls for that user (for example, the query request) will be denied.

> **Important**
>
> Inadvertent mistakes when you update the User Store's user, group, group membership, and mapping information can result in unintentional and unacceptable changes in the accessibility of documents to users.
> Treat the ability to update the User Store to create users, update users, delete users, create groups, update groups, delete groups (i.e, create update delete operations), and update the mappings, as a privileged operation.
> Ensure that access to the User Store APIs is provided only to admin who fully understand how to use these APIs and the implications of these changes on your document security.
> We recommend establishing a documented approval process for making such changes.

Sync scope

You can choose to customize the content crawled and indexed by your data source connector. The sync scope options available vary based on the data source connector.

Document deletion safeguard

You can protect your documents from accidental deletion during sync by setting a **Document deletion safeguard**, a maximum document deletion percentage. Setting a maximum document deletion percentage prevents your indexed files from accidental excessive deletion and accidental data loss due to issues such as crawler failures and temporary data source unavailability.

The **Document deletion safeguard** is calculated in the beginning of the crawl process during a sync job. The formula is 100*(document to be deleted)/(document scanned + to be deleted). If the number of documents to be deleted exceeds the configured threshold percentage, the delete phase will be skipped during a sync job, and no documents will be deleted from the index. The data source sync job will still sync and index the new and modified content.

You set a **Document deletion safeguard** during data source configuration in **Sync scope**. A value of 0% means that no documents from this data source will be deleted from your index. A value of 100% allows unlimited deletion during the sync process, meaning no deletion protection.

You can view the number of documents protected from deletion during a sync job in the **Protected from deletion** column in **Sync run history**. The number in the column is a hyperlink to CloudWatch where you can view additional information and run queries.

Sync mode

With sync mode, you can customize what content gets synced with your index when your data source content changes. Choose from the following options:

Console

- **Full sync** – Sync all content regardless of the previous sync status.
- **New or modified content sync** – Sync only new or modified documents.
- **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.
- **Change log** – Crawl and sync only new, modified, and deleted content.

API

Specify the sync mode using the `configuration` parameter of the CreateDataSource operation. Choose from the following options:

- **Forced full crawl** – Crawl and sync all content to your index.
- **Full crawl** – Crawl all content and sync only new, modified, or deleted content.
- **Change log** – Crawl and sync only new, modified, and deleted content.

> **Note**
>
> Available sync mode features vary across data source connectors.

> **Important**
>
> If you get a Resource not found exception when you try to view your CloudWatch logs for a data source sync job in progress, it's because the CloudWatch logs aren't available yet. Wait for some time and check again.

Sync run schedule

When you use the console or the CreateDataSource API operation, you can choose to periodically sync your data source with your retriever on a custom schedule. You can choose from the following frequency options:

- **Run on demand** – Sync a data source with your index only when you choose to.
- **Hourly** – Sync your data source with your index every hour. You can choose which minute the sync begins.
- **Daily** – Sync your data source with your index daily. You can choose the sync start time in UTC format in hours and minutes.
- **Weekly** – Sync your data source with your index weekly. You can choose the days to sync and the sync start time in hours and minutes (UTC format).
- **Monthly** – Sync your data source monthly with your index. You can choose the day of the month to start the sync and the sync start time in hours and minutes (UTC format).
- **Custom** – Sync your data source to your index using a cron expression. A cron expression is a string comprising five or six required fields, separated by white space. Cron expressions represent a set of times programmed to schedule events. For example, an expression to activate a rule every day at 12:00pm UTC can look like: `(0 12 * * ? *)`. Similarly, an expression to activate a rule every day at 10:15am UTC on the last Friday of each month during the years 2023 to 2025 can look like: `(15 10 ? * 6L 2023-2025)`.

> **Note**
>
> Amazon Q Business will not sync the data source (even for the first time) until you select **Sync now** after you successfully add the data source.

Field mappings

When you connect Amazon Q Business to your data, your data source connector crawls relevant metadata or attributes associated with a document. Examples of metadata include date of creation, document id, and document name. Then, Amazon Q maps the metadata to fields within your Amazon Q Business index.

You map data source document attributes to Amazon Q Business index fields using the **Field mappings** feature on the console, or the `configuration` parameter of the `CreateDataSource`

API operation. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application environment and retriever are created.

Document attributes need to be enabled for search before they can be used to customize end user chat experience. To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q. To learn how to enable document attributes for search, see Configuring metadata controls in Amazon Q.

All fields and attributes have a size limit of 2048 characters. Fields or attributes longer than this value are truncated before document ingestion.

For more information, see the following topics:

- Document attributes and types
- Filtering using metadata

What is a document?

When you connect Amazon Q Business to a data source, what Amazon Q Business considers—and crawls—as a document varies by connector.

The following table outlines what each connector crawls as a document.

Data source connector	Supports crawling	Document definition
Adobe Experience Manager (Cloud and Server)	• Assets • Pages	• Each Asset is considered a single document. • Each Page is considered a single document.
Alfresco (Cloud and Server)	• Files • Comments	• Each File is considered a single document. • Each Comment is considered a single document.

Data source connector	Supports crawling	Document definition
Amazon FSx (Windows)	Files	Each File is considered a single document.
Amazon S3	Objects	Each Object is considered a single document. Any *object-name.metadata.json* file and access control list (ACL) file is considered metadata for the object it is associated with and not treated as a separate document.
Amazon Q Business Web Crawler	• Web pages • Attachments	• Each Web page is considered a single document. • Each Attachment is considered a single document.
WorkDocs	• Files • Comments	• Each File is considered a single document. • Each Comment is considered a single document.
Box	• Files • Tasks • Comments • Weblinks	• Each File is considered a single document. • Each Task is considered a single document. • Each Comment is considered a single document. • Each Weblink is considered a single document.

Data source connector	Supports crawling	Document definition
Confluence (Cloud and Server)	• Spaces • Pages • Blogs • Comments • Attachments	• Each Space is considered a single document. • Each Page is considered a single document. • Each Blog is considered a single document. • Each Comment is considered a single document. • Each Attachment is considered a single document.
Database data sources • Aurora (MySQL) • Aurora (PostgreSQL • Amazon RDS (Microsoft SQL Server) • Amazon RDS (MySQL) • Amazon RDS (Oracle) • Amazon RDS (PostgreSQL) • IBM DB2 • PostgreSQL • Microsoft SQL Server • MySQL • Oracle Database	• Table data in a single database • View data in a single database	Each row in a table and view is considered a single document.

Data source connector	Supports crawling	Document definition
Dropbox	• Files • Papers • Paper templates • Shortcuts	• Each File is considered a single document. • Each Paper is considered a single document. • Each Paper template is considered a single document. • Each Shortcut is considered a single document.
Drupal	• Articles • Basic pages • Basic blocks • Custom content • Custom blocks • Comments on articles, basic pages, basic blocks, custom content, and custom blocks • Attachments in articles, basic pages, basic blocks, custom content, and custom blocks	• Each Article is considered a single document. • Each Basic page is considered a single document. • Each Basic block is considered a single document. • Each Custom content is considered a single document. • Each Custom block is considered a single document. • Each Comment on an article, a basic page, a basic block, any custom content, and a custom block is considered a document. • Each Attachment in an article, a basic page, a basic block, any custom content, and a custom block is considered a document.

Data source connector	Supports crawling	Document definition
GitHub (Cloud and Server)	• Respositories • Repository commits • Issues • Issue attachments • Issue comments • Pull request documents • Pull request comments • Pull request attachments	• Each Repository is considered a single document. • Each Repository commit is considered a single document. • Each Issue is considered a single document. • Each Issue attachmen t is considered a single document. • Each Issue comment is considered a single document. • Each Pull request is considered a single document. • Each Pull request comment is considered a single document. • Each Pull request attachment is considered a single document.
Gmail	• Emails • Email attachments	• Each Email is considered a single document. • Each Email attachmen t is considered a single document.
Google Calendar	• Calendar	Each calendar is considered a single document.

Data source connector	Supports crawling	Document definition
Google Drive	• Files • Comments	• Each File is considered a single document. • Each Comment is considered a single document.
Jira	• Projects • Issues • Comments • Attachments • Worklog	• Each Project is considered a single document. • Each Issue is considered a single document. • Each Comment is considered a single document. • Each Attachment is considered a single document. • Each Worklog is considered a single document.
Microsoft Exchange	• Emails • Attachments • Calendar • Contacts • Notes • OneNotes	• Each Email is considered a single document. • Each Attachment is considered a single document. • Each Calendar is considered a single document. • Each Contact is considered a single document. • Each Note is considered a single document. • Each page in OneNotes is considered a single document.

Data source connector	Supports crawling	Document definition
Microsoft OneDrive	• Files • OneNotes	• Each File is considered a single document. • Each page in OneNotes is considered a single document.
Microsoft SharePoint (Online and Server)	• Events • Pages • Files • Links • File attachments • Comments • OneNotes	• Each Event is considered a single document. • Each Page is considered a single document. • Each File is considered a single document. • Each Link is considered a single document. • Each File attachment is considered a single document. • Each Comment is considered a single document. • Each page in OneNotes is considered a single document.

Data source connector	Supports crawling	Document definition
Microsoft Teams	• Chat messages • Chat attachments • Channel posts • Channel wikis • Channel attachments • Meeting chats • Meeting files • Meeting notes • Calendar meetings • OneNotes	• Each Chat message is considered a single document. • Each Chat attachmen t is considered a single document. • Each Channel post is considered a single document. • Each Channel wiki is considered a single document. • Each Channel attachmen t is considered a single document. • Each Meeting chat is considered a single document. • Each Meeting file is considered a single document. • Each Meeting note is considered a single document. • Each Calendar meeting is considered a single document. • Each page in OneNotes is considered a single document.

Data source connector	Supports crawling	Document definition
Microsoft Yammer	• Communities • Attachments • Messages • Users	• Each Community is considered a single document. • Each Attachment is considered a single document. • Each Message and community post is considered a single document. • Each User is considered a single document.
Quip	• Files • Messages • Threads	• Each File is considered a single document. • Each Comment is considered a single document. • Each file and message posted in a Thread is considered a single document.

Data source connector	Supports crawling	Document definition
Salesforce	• Accounts • Contacts • Campaigns • Contracts • Cases • Partners • Opportunities • Groups • Leads • Users • Tasks • Ideas • Profiles • Solutions • Chatters • Documents • Custom entities • Knowledge articles	• Each Account is considered a single document. • Each Contact is considered a single document. • Each Campaign is considere d a single document. • Each Contract is considered a single document. • Each Case is considered a single document. • Each Partner is considered a single document. • Each Opportunity is considered a single document. • Each Group is considered a single document. • Each Lead is considered a single document. • Each User is considered a single document. • Each Task is considered a single document. • Each Idea is considered a single document. • Each Profile is considered a single document. • Each Solution is considered a single document. • Each Chatter is considered a single document.

Data source connector	Supports crawling	Document definition
		• Each Document (file) is considered a single document. • Each Custom entity (record) is considered a single document. • Each Knowledge article is considered a single document.
ServiceNow	• Incidents • Knowledge articles • Service catalog • Attachments	• Each Incident is considered a single document. • Each Knowledge article is considered a single document. • Each Service catalog is considered a single document. • Each Attachment is considered a single document.
Slack	• Messages • Message attachments • Channel posts	• Each Message is considered a single document. • Each Message attachmen t is considered a single document. • Each Channel post is considered a single document.

Data source connector	Supports crawling	Document definition
Zendesk	• Tickets • Ticket comments • Ticket comment attachments • Articles • Article attachments • Article comments • Community topics • Community posts • Community post comments	• Each Ticket is considered a single document. • Each Ticket comment is considered a single document. • Each Ticket comment attachment is considered a single document. • Each Article is considered a single document. • Each Article attachment is considered a single document. • Each Article comment is considered a single document. • Each Community topic is considered a single document. • Each Community post is considered a single document. • Each Community post comment is considered a single document.

Best practices for data source connector configuration in Amazon Q Business

The following list describes best practices for setting up and configuring your Amazon Q Business data source connector:

- Each document in an index must be unique. Check that there are no duplicate documents in a data source, or across any data sources, that you plan to connect to an Amazon Q Business retriever.
- If you change your authentication type and credentials, you must update your IAM role to access the correct AWS Secrets Manager secret ID.
- We recommend that you regularly refresh or rotate your credentials and secret. Provide only the necessary access level for your own security. We don't recommend the re-use of credentials and secrets across data sources.
- IAM roles used for retrievers can't be used for data sources. If you're unsure if an existing role is used for a retriever or data source, create a new IAM role to avoid errors.
- If your application uses AWS KMS keys, ensure that the IAM role associated with your application environment has permission to describe the key, and to encrypt and decrypt data using it.
- For on-premises or server data source connectors, Amazon Q Business checks if the endpoint information included in Secrets Manager is the same as the endpoint information specified in your data source configuration details. This helps protect against the confused deputy problem, which is a security issue. The problem occurs when a user doesn't have permission to perform an action. But, by using Amazon Q Business as a proxy, the user can access the configured secret and perform the action.

  If you change your endpoint information later, you must create a new secret to sync this information.
- Most data sources use regular expression patterns, which are inclusion or exclusion patterns referred to as *filters*.

  If you specify an inclusion filter, only content that matches the inclusion filter is indexed. If you specify an inclusion and exclusion filter, documents that match the exclusion filter aren't indexed, even if they match the inclusion filter.

Supported connectors

Amazon Q Business supports the following connectors:

- Amazon Q Business custom data source connector
- Amazon Q Web Crawler
- Asana (*Preview*)
- Box

- Confluence (Cloud)
- Confluence (Server)
- Dropbox
- Amazon FSx Windows
- GitHub (Cloud)
- GitHub (Server)
- Gmail
- Google Calendar (*Preview*)
- Google Drive
- Jira
- Microsoft Exchange
- Microsoft OneDrive
- Microsoft SharePoint (Cloud)
- Microsoft SharePoint Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server (Subscription Edition)
- Microsoft Teams
- Amazon S3
- Salesforce Online
- ServiceNow Online
- Slack
- Smartsheet
- Zendesk

Legacy connectors

The following connectors remain supported for existing customers but are no longer available for new onboarding. Support for existing usage will continue until May 31, 2026:

- AEM (Cloud)

- AEM (Server)
- Alfresco (Cloud)
- Alfresco (Server)
- Aurora (MySQL)
- Aurora (PostgreSQL)
- Drupal
- IBM DB2
- Microsoft SQL Server
- Microsoft Yammer
- MySQL
- Oracle Database
- PostgreSQL
- Quip
- Amazon RDS (Microsoft SQL Server)
- Amazon RDS (MySQL)
- Amazon RDS (Oracle)
- Amazon RDS (PostgreSQL)

Connecting AEM (Cloud) to Amazon Q Business

> **Note**
>
> AEM (Cloud) connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Adobe Experience Manager (AEM) is a content management system (CMS) that's used for creating website or mobile app content. You can connect your AEM (Cloud) instance to Amazon Q Business

—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the Amazon Q Business AEM (Cloud) connector
- AEM (Cloud) connector overview
- Prerequisites for connecting Amazon Q Business to AEM (Cloud)
- Connecting Amazon Q Business to AEM (Cloud) using the console
- Connecting Amazon Q Business to AEM (Cloud) using APIs
- How Amazon Q Business connector crawls AEM (Cloud) ACLs
- Amazon Q Business AEM (Cloud) data source connector field mappings
- IAM role for Amazon Q AEM (Cloud) connector
- Understand error codes in the AEM (Cloud) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Amazon Q Business AEM (Cloud) connector

The AEM (Cloud) connector has the following known limitations:

- Deleted site pages can't be tracked when you use **Change log** sync or **Sync only new, modified, or deleted document sync**.

AEM (Cloud) connector overview

The following table gives an overview of the Amazon Q Business AEM (Cloud) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic, OAuth 2.0 with Client Credentials Flow
	Authentication credentials	**Basic** • AEM (Cloud) host URL • Username of AEM user • Password of AEM user **OAuth 2.0 with Client Credentials Flow** • AEM (Cloud) host URL • Client ID • Client secret • Private key • Organization ID • Technical Account ID • Adobe Identity Management System (IMS) host **Important** Admin privileges required.
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported:

Category	Feature	Support
		• Pages • Assets See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include/exclude by asset name • Include/exclude by asset type • Include/exclude by asset path • Include/exclude by page name • Include/exclude by page path
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to AEM (Cloud)

Before you begin, make sure that you have completed the following prerequisites.

In AEM, make sure you have:

- Access to an account with administrative permissions, or are an admin user.
- Copied your AEM (Cloud) host URL.
- Noted your basic authentication credentials of admin username and password.
- (Optional) Added the following OAuth scopes if you're using OAuth 2.0 authentication:
  - **Profile** – Needed to get user and groups related data, like email ID and username.
  - **Replicate** – Needed to get data and metadata from Assets and Pages (not including user data).

- **Optional**: Generated OAuth 2.0 credentials in AEM (Cloud) as an admin user. The credentials include client ID, client secret, private key, organization ID, technical account ID, and Adobe Identity Management System (IMS) host. For more information about how to generate these credentials for AEM (Cloud), see AEM (Cloud) documentation.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your AEM (Cloud) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to AEM (Cloud) using the console

The following procedure outlines how to connect Amazon Q Business to AEM (Cloud) using the AWS Management Console.

Connecting Amazon Q to AEM (Cloud)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Adobe Experience Manager** data source to your Amazon Q application.
5. Then, on the **AEM (Cloud)** data source page, enter the following information:
6. **Name and description**, do the following:

- For **Data source name** – Name your data source for easy tracking.

> **Note**
>
> You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. **Source** – Choose **AEM as a Cloud Service**.

   - **AEM host URL** – Enter your **AEM host URL**. If you use AEM as a Cloud Service, you can use the author URL. For example: *`https://author-xxxxx-xxxxxx-adobeaemcloud.com`*.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. **Authentication** – Choose between **Basic authentication** and **OAuth 2.0 authentication** and then enter the following information for your **AWS Secrets Manager secret**.

   a. **Basic authentication** – Enter a name for the secret, your AEM site admin username, and admin password.

   b. **OAuth 2.0 authentication** – Enter a name for the secret, your client ID, client secret, private key, organization ID, technical account ID, and Adobe IMS host.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **Identity crawler** – Amazon Q crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.
12. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.
13. In **Sync scope**, enter the following information:

    a. **Sync content types** – Choose whether to crawl only **Pages** or **Assets**, or both.

    b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

    c. **Additional configuration – *optional*** – Configure the following settings:

    - **Page components** – The specific names of page components. The Page Component is an extensible page component designed to work with the Adobe AEM template editor and allows page header and footer and structure components to be assembled with the template editor.
    - **Content fragment variations** – The specific names of content fragment variations. Content Fragments allow you to design, create, curate, and publish page-independent content in Adobe AEM. They allow you to prepare content ready for use in multiple locations and over multiple channels.
    - **Root paths** – The root paths to specific content.
    - **Regex patterns** – The regular expression patterns to include or exclude certain pages and assets.

    d. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete

phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New or modified content sync** – Sync only new and modified documents.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

    For more details, see Sync mode.

15. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
16. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
17. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

    For more information, see Field mappings.

18. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to AEM (Cloud) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

AEM JSON schema

The following is the AEM JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
```

```
            "aemUrl": {
              "type": "string",
              "pattern": "https:.*"
            },
            "authType": {
              "type": "string",
              "enum": [
                "Basic",
                "OAuth2"
              ]
            },
            "deploymentType": {
              "type": "string",
              "enum": [
                "CLOUD",
                "ON_PREMISE"
              ]
            }
          },
          "required": [
            "aemUrl",
            "authType",
            "deploymentType"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "page": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
```

```
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": [
                    "STRING",
                    "STRING_LIST",
                    "DATE",
                    "LONG"
                  ]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "asset": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
```

```
                    "type": "string",
                    "enum": [
                      "STRING",
                      "STRING_LIST",
                      "DATE",
                      "LONG"
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "isCrawlAcl": {
        "type": "boolean"
      },
      "fieldForUserId": {
        "type": "string"
      },
      "timeZoneId": {
        "type": "string",
        "enum": [
          "Africa/Abidjan",
```

```
            "Africa/Accra",
            "Africa/Addis_Ababa",
            "Africa/Algiers",
            "Africa/Asmara",
            "Africa/Asmera",
            "Africa/Bamako",
            "Africa/Bangui",
            "Africa/Banjul",
            "Africa/Bissau",
            "Africa/Blantyre",
            "Africa/Brazzaville",
            "Africa/Bujumbura",
            "Africa/Cairo",
            "Africa/Casablanca",
            "Africa/Ceuta",
            "Africa/Conakry",
            "Africa/Dakar",
            "Africa/Dar_es_Salaam",
            "Africa/Djibouti",
            "Africa/Douala",
            "Africa/El_Aaiun",
            "Africa/Freetown",
            "Africa/Gaborone",
            "Africa/Harare",
            "Africa/Johannesburg",
            "Africa/Juba",
            "Africa/Kampala",
            "Africa/Khartoum",
            "Africa/Kigali",
            "Africa/Kinshasa",
            "Africa/Lagos",
            "Africa/Libreville",
            "Africa/Lome",
            "Africa/Luanda",
            "Africa/Lubumbashi",
            "Africa/Lusaka",
            "Africa/Malabo",
            "Africa/Maputo",
            "Africa/Maseru",
            "Africa/Mbabane",
            "Africa/Mogadishu",
            "Africa/Monrovia",
            "Africa/Nairobi",
            "Africa/Ndjamena",
```

```
            "Africa/Niamey",
            "Africa/Nouakchott",
            "Africa/Ouagadougou",
            "Africa/Porto-Novo",
            "Africa/Sao_Tome",
            "Africa/Timbuktu",
            "Africa/Tripoli",
            "Africa/Tunis",
            "Africa/Windhoek",
            "America/Adak",
            "America/Anchorage",
            "America/Anguilla",
            "America/Antigua",
            "America/Araguaina",
            "America/Argentina/Buenos_Aires",
            "America/Argentina/Catamarca",
            "America/Argentina/ComodRivadavia",
            "America/Argentina/Cordoba",
            "America/Argentina/Jujuy",
            "America/Argentina/La_Rioja",
            "America/Argentina/Mendoza",
            "America/Argentina/Rio_Gallegos",
            "America/Argentina/Salta",
            "America/Argentina/San_Juan",
            "America/Argentina/San_Luis",
            "America/Argentina/Tucuman",
            "America/Argentina/Ushuaia",
            "America/Aruba",
            "America/Asuncion",
            "America/Atikokan",
            "America/Atka",
            "America/Bahia",
            "America/Bahia_Banderas",
            "America/Barbados",
            "America/Belem",
            "America/Belize",
            "America/Blanc-Sablon",
            "America/Boa_Vista",
            "America/Bogota",
            "America/Boise",
            "America/Buenos_Aires",
            "America/Cambridge_Bay",
            "America/Campo_Grande",
            "America/Cancun",
```

```
            "America/Caracas",
            "America/Catamarca",
            "America/Cayenne",
            "America/Cayman",
            "America/Chicago",
            "America/Chihuahua",
            "America/Ciudad_Juarez",
            "America/Coral_Harbour",
            "America/Cordoba",
            "America/Costa_Rica",
            "America/Creston",
            "America/Cuiaba",
            "America/Curacao",
            "America/Danmarkshavn",
            "America/Dawson",
            "America/Dawson_Creek",
            "America/Denver",
            "America/Detroit",
            "America/Dominica",
            "America/Edmonton",
            "America/Eirunepe",
            "America/El_Salvador",
            "America/Ensenada",
            "America/Fort_Nelson",
            "America/Fort_Wayne",
            "America/Fortaleza",
            "America/Glace_Bay",
            "America/Godthab",
            "America/Goose_Bay",
            "America/Grand_Turk",
            "America/Grenada",
            "America/Guadeloupe",
            "America/Guatemala",
            "America/Guayaquil",
            "America/Guyana",
            "America/Halifax",
            "America/Havana",
            "America/Hermosillo",
            "America/Indiana/Indianapolis",
            "America/Indiana/Knox",
            "America/Indiana/Marengo",
            "America/Indiana/Petersburg",
            "America/Indiana/Tell_City",
            "America/Indiana/Vevay",
```

```
            "America/Indiana/Vincennes",
            "America/Indiana/Winamac",
            "America/Indianapolis",
            "America/Inuvik",
            "America/Iqaluit",
            "America/Jamaica",
            "America/Jujuy",
            "America/Juneau",
            "America/Kentucky/Louisville",
            "America/Kentucky/Monticello",
            "America/Knox_IN",
            "America/Kralendijk",
            "America/La_Paz",
            "America/Lima",
            "America/Los_Angeles",
            "America/Louisville",
            "America/Lower_Princes",
            "America/Maceio",
            "America/Managua",
            "America/Manaus",
            "America/Marigot",
            "America/Martinique",
            "America/Matamoros",
            "America/Mazatlan",
            "America/Mendoza",
            "America/Menominee",
            "America/Merida",
            "America/Metlakatla",
            "America/Mexico_City",
            "America/Miquelon",
            "America/Moncton",
            "America/Monterrey",
            "America/Montevideo",
            "America/Montreal",
            "America/Montserrat",
            "America/Nassau",
            "America/New_York",
            "America/Nipigon",
            "America/Nome",
            "America/Noronha",
            "America/North_Dakota/Beulah",
            "America/North_Dakota/Center",
            "America/North_Dakota/New_Salem",
            "America/Nuuk",
```

```
            "America/Ojinaga",
            "America/Panama",
            "America/Pangnirtung",
            "America/Paramaribo",
            "America/Phoenix",
            "America/Port-au-Prince",
            "America/Port_of_Spain",
            "America/Porto_Acre",
            "America/Porto_Velho",
            "America/Puerto_Rico",
            "America/Punta_Arenas",
            "America/Rainy_River",
            "America/Rankin_Inlet",
            "America/Recife",
            "America/Regina",
            "America/Resolute",
            "America/Rio_Branco",
            "America/Rosario",
            "America/Santa_Isabel",
            "America/Santarem",
            "America/Santiago",
            "America/Santo_Domingo",
            "America/Sao_Paulo",
            "America/Scoresbysund",
            "America/Shiprock",
            "America/Sitka",
            "America/St_Barthelemy",
            "America/St_Johns",
            "America/St_Kitts",
            "America/St_Lucia",
            "America/St_Thomas",
            "America/St_Vincent",
            "America/Swift_Current",
            "America/Tegucigalpa",
            "America/Thule",
            "America/Thunder_Bay",
            "America/Tijuana",
            "America/Toronto",
            "America/Tortola",
            "America/Vancouver",
            "America/Virgin",
            "America/Whitehorse",
            "America/Winnipeg",
            "America/Yakutat",
```

```
            "America/Yellowknife",
            "Antarctica/Casey",
            "Antarctica/Davis",
            "Antarctica/DumontDUrville",
            "Antarctica/Macquarie",
            "Antarctica/Mawson",
            "Antarctica/McMurdo",
            "Antarctica/Palmer",
            "Antarctica/Rothera",
            "Antarctica/South_Pole",
            "Antarctica/Syowa",
            "Antarctica/Troll",
            "Antarctica/Vostok",
            "Arctic/Longyearbyen",
            "Asia/Aden",
            "Asia/Almaty",
            "Asia/Amman",
            "Asia/Anadyr",
            "Asia/Aqtau",
            "Asia/Aqtobe",
            "Asia/Ashgabat",
            "Asia/Ashkhabad",
            "Asia/Atyrau",
            "Asia/Baghdad",
            "Asia/Bahrain",
            "Asia/Baku",
            "Asia/Bangkok",
            "Asia/Barnaul",
            "Asia/Beirut",
            "Asia/Bishkek",
            "Asia/Brunei",
            "Asia/Calcutta",
            "Asia/Chita",
            "Asia/Choibalsan",
            "Asia/Chongqing",
            "Asia/Chungking",
            "Asia/Colombo",
            "Asia/Dacca",
            "Asia/Damascus",
            "Asia/Dhaka",
            "Asia/Dili",
            "Asia/Dubai",
            "Asia/Dushanbe",
            "Asia/Famagusta",
```

```
            "Asia/Gaza",
            "Asia/Harbin",
            "Asia/Hebron",
            "Asia/Ho_Chi_Minh",
            "Asia/Hong_Kong",
            "Asia/Hovd",
            "Asia/Irkutsk",
            "Asia/Istanbul",
            "Asia/Jakarta",
            "Asia/Jayapura",
            "Asia/Jerusalem",
            "Asia/Kabul",
            "Asia/Kamchatka",
            "Asia/Karachi",
            "Asia/Kashgar",
            "Asia/Kathmandu",
            "Asia/Katmandu",
            "Asia/Khandyga",
            "Asia/Kolkata",
            "Asia/Krasnoyarsk",
            "Asia/Kuala_Lumpur",
            "Asia/Kuching",
            "Asia/Kuwait",
            "Asia/Macao",
            "Asia/Macau",
            "Asia/Magadan",
            "Asia/Makassar",
            "Asia/Manila",
            "Asia/Muscat",
            "Asia/Nicosia",
            "Asia/Novokuznetsk",
            "Asia/Novosibirsk",
            "Asia/Omsk",
            "Asia/Oral",
            "Asia/Phnom_Penh",
            "Asia/Pontianak",
            "Asia/Pyongyang",
            "Asia/Qatar",
            "Asia/Qostanay",
            "Asia/Qyzylorda",
            "Asia/Rangoon",
            "Asia/Riyadh",
            "Asia/Saigon",
            "Asia/Sakhalin",
```

```
            "Asia/Samarkand",
            "Asia/Seoul",
            "Asia/Shanghai",
            "Asia/Singapore",
            "Asia/Srednekolymsk",
            "Asia/Taipei",
            "Asia/Tashkent",
            "Asia/Tbilisi",
            "Asia/Tehran",
            "Asia/Tel_Aviv",
            "Asia/Thimbu",
            "Asia/Thimphu",
            "Asia/Tokyo",
            "Asia/Tomsk",
            "Asia/Ujung_Pandang",
            "Asia/Ulaanbaatar",
            "Asia/Ulan_Bator",
            "Asia/Urumqi",
            "Asia/Ust-Nera",
            "Asia/Vientiane",
            "Asia/Vladivostok",
            "Asia/Yakutsk",
            "Asia/Yangon",
            "Asia/Yekaterinburg",
            "Asia/Yerevan",
            "Atlantic/Azores",
            "Atlantic/Bermuda",
            "Atlantic/Canary",
            "Atlantic/Cape_Verde",
            "Atlantic/Faeroe",
            "Atlantic/Faroe",
            "Atlantic/Jan_Mayen",
            "Atlantic/Madeira",
            "Atlantic/Reykjavik",
            "Atlantic/South_Georgia",
            "Atlantic/St_Helena",
            "Atlantic/Stanley",
            "Australia/ACT",
            "Australia/Adelaide",
            "Australia/Brisbane",
            "Australia/Broken_Hill",
            "Australia/Canberra",
            "Australia/Currie",
            "Australia/Darwin",
```

```
            "Australia/Eucla",
            "Australia/Hobart",
            "Australia/LHI",
            "Australia/Lindeman",
            "Australia/Lord_Howe",
            "Australia/Melbourne",
            "Australia/NSW",
            "Australia/North",
            "Australia/Perth",
            "Australia/Queensland",
            "Australia/South",
            "Australia/Sydney",
            "Australia/Tasmania",
            "Australia/Victoria",
            "Australia/West",
            "Australia/Yancowinna",
            "Brazil/Acre",
            "Brazil/DeNoronha",
            "Brazil/East",
            "Brazil/West",
            "CET",
            "CST6CDT",
            "Canada/Atlantic",
            "Canada/Central",
            "Canada/Eastern",
            "Canada/Mountain",
            "Canada/Newfoundland",
            "Canada/Pacific",
            "Canada/Saskatchewan",
            "Canada/Yukon",
            "Chile/Continental",
            "Chile/EasterIsland",
            "Cuba",
            "EET",
            "EST5EDT",
            "Egypt",
            "Eire",
            "Etc/GMT",
            "Etc/GMT+0",
            "Etc/GMT+1",
            "Etc/GMT+10",
            "Etc/GMT+11",
            "Etc/GMT+12",
            "Etc/GMT+2",
```

```
            "Etc/GMT+3",
            "Etc/GMT+4",
            "Etc/GMT+5",
            "Etc/GMT+6",
            "Etc/GMT+7",
            "Etc/GMT+8",
            "Etc/GMT+9",
            "Etc/GMT-0",
            "Etc/GMT-1",
            "Etc/GMT-10",
            "Etc/GMT-11",
            "Etc/GMT-12",
            "Etc/GMT-13",
            "Etc/GMT-14",
            "Etc/GMT-2",
            "Etc/GMT-3",
            "Etc/GMT-4",
            "Etc/GMT-5",
            "Etc/GMT-6",
            "Etc/GMT-7",
            "Etc/GMT-8",
            "Etc/GMT-9",
            "Etc/GMT0",
            "Etc/Greenwich",
            "Etc/UCT",
            "Etc/UTC",
            "Etc/Universal",
            "Etc/Zulu",
            "Europe/Amsterdam",
            "Europe/Andorra",
            "Europe/Astrakhan",
            "Europe/Athens",
            "Europe/Belfast",
            "Europe/Belgrade",
            "Europe/Berlin",
            "Europe/Bratislava",
            "Europe/Brussels",
            "Europe/Bucharest",
            "Europe/Budapest",
            "Europe/Busingen",
            "Europe/Chisinau",
            "Europe/Copenhagen",
            "Europe/Dublin",
            "Europe/Gibraltar",
```

```
            "Europe/Guernsey",
            "Europe/Helsinki",
            "Europe/Isle_of_Man",
            "Europe/Istanbul",
            "Europe/Jersey",
            "Europe/Kaliningrad",
            "Europe/Kiev",
            "Europe/Kirov",
            "Europe/Kyiv",
            "Europe/Lisbon",
            "Europe/Ljubljana",
            "Europe/London",
            "Europe/Luxembourg",
            "Europe/Madrid",
            "Europe/Malta",
            "Europe/Mariehamn",
            "Europe/Minsk",
            "Europe/Monaco",
            "Europe/Moscow",
            "Europe/Nicosia",
            "Europe/Oslo",
            "Europe/Paris",
            "Europe/Podgorica",
            "Europe/Prague",
            "Europe/Riga",
            "Europe/Rome",
            "Europe/Samara",
            "Europe/San_Marino",
            "Europe/Sarajevo",
            "Europe/Saratov",
            "Europe/Simferopol",
            "Europe/Skopje",
            "Europe/Sofia",
            "Europe/Stockholm",
            "Europe/Tallinn",
            "Europe/Tirane",
            "Europe/Tiraspol",
            "Europe/Ulyanovsk",
            "Europe/Uzhgorod",
            "Europe/Vaduz",
            "Europe/Vatican",
            "Europe/Vienna",
            "Europe/Vilnius",
            "Europe/Volgograd",
```

```
            "Europe/Warsaw",
            "Europe/Zagreb",
            "Europe/Zaporozhye",
            "Europe/Zurich",
            "GB",
            "GB-Eire",
            "GMT",
            "GMT0",
            "Greenwich",
            "Hongkong",
            "Iceland",
            "Indian/Antananarivo",
            "Indian/Chagos",
            "Indian/Christmas",
            "Indian/Cocos",
            "Indian/Comoro",
            "Indian/Kerguelen",
            "Indian/Mahe",
            "Indian/Maldives",
            "Indian/Mauritius",
            "Indian/Mayotte",
            "Indian/Reunion",
            "Iran",
            "Israel",
            "Jamaica",
            "Japan",
            "Kwajalein",
            "Libya",
            "MET",
            "MST7MDT",
            "Mexico/BajaNorte",
            "Mexico/BajaSur",
            "Mexico/General",
            "NZ",
            "NZ-CHAT",
            "Navajo",
            "PRC",
            "PST8PDT",
            "Pacific/Apia",
            "Pacific/Auckland",
            "Pacific/Bougainville",
            "Pacific/Chatham",
            "Pacific/Chuuk",
            "Pacific/Easter",
```

```
            "Pacific/Efate",
            "Pacific/Enderbury",
            "Pacific/Fakaofo",
            "Pacific/Fiji",
            "Pacific/Funafuti",
            "Pacific/Galapagos",
            "Pacific/Gambier",
            "Pacific/Guadalcanal",
            "Pacific/Guam",
            "Pacific/Honolulu",
            "Pacific/Johnston",
            "Pacific/Kanton",
            "Pacific/Kiritimati",
            "Pacific/Kosrae",
            "Pacific/Kwajalein",
            "Pacific/Majuro",
            "Pacific/Marquesas",
            "Pacific/Midway",
            "Pacific/Nauru",
            "Pacific/Niue",
            "Pacific/Norfolk",
            "Pacific/Noumea",
            "Pacific/Pago_Pago",
            "Pacific/Palau",
            "Pacific/Pitcairn",
            "Pacific/Pohnpei",
            "Pacific/Ponape",
            "Pacific/Port_Moresby",
            "Pacific/Rarotonga",
            "Pacific/Saipan",
            "Pacific/Samoa",
            "Pacific/Tahiti",
            "Pacific/Tarawa",
            "Pacific/Tongatapu",
            "Pacific/Truk",
            "Pacific/Wake",
            "Pacific/Wallis",
            "Pacific/Yap",
            "Poland",
            "Portugal",
            "ROK",
            "Singapore",
            "SystemV/AST4",
            "SystemV/AST4ADT",
```

```
            "SystemV/CST6",
            "SystemV/CST6CDT",
            "SystemV/EST5",
            "SystemV/EST5EDT",
            "SystemV/HST10",
            "SystemV/MST7",
            "SystemV/MST7MDT",
            "SystemV/PST8",
            "SystemV/PST8PDT",
            "SystemV/YST9",
            "SystemV/YST9YDT",
            "Turkey",
            "UCT",
            "US/Alaska",
            "US/Aleutian",
            "US/Arizona",
            "US/Central",
            "US/East-Indiana",
            "US/Eastern",
            "US/Hawaii",
            "US/Indiana-Starke",
            "US/Michigan",
            "US/Mountain",
            "US/Pacific",
            "US/Samoa",
            "UTC",
            "Universal",
            "W-SU",
            "WET",
            "Zulu",
            "EST",
            "HST",
            "MST",
            "ACT",
            "AET",
            "AGT",
            "ART",
            "AST",
            "BET",
            "BST",
            "CAT",
            "CNT",
            "CST",
            "CTT",
```

```
            "EAT",
            "ECT",
            "IET",
            "IST",
            "JST",
            "MIT",
            "NET",
            "NST",
            "PLT",
            "PNT",
            "PRT",
            "PST",
            "SST",
            "VST"
          ]
        },
        "pageRootPaths": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "assetRootPaths": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "crawlAssets": {
          "type": "boolean"
        },
        "crawlPages": {
          "type": "boolean"
        },
        "pagePathInclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "pagePathExclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
```

```
          }
        },
        "pageNameInclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "pageNameExclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "assetPathInclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "assetPathExclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "assetTypeInclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "assetTypeExclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "assetNameInclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
```

```
        "assetNameExclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "pageComponents": {
          "type": "array",
          "items": {
            "type": "object"
          }
        },
        "contentFragmentVariations": {
          "type": "array",
          "items": {
            "type": "object"
          }
        },
        "cugExemptedPrincipals": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        }
      },
      "required": []
    },
    "type": {
      "type": "string",
      "pattern": "AEM"
    },
    "enableIdentityCrawler": {
      "type": "boolean"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
```

```
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the endpoint for the data source.
`repositoryEndpointMetadata`	The endpoint information for the data source.
`aemUrl`	The Adobe Experience Manager host URL. For example, if you use AEM On-Premise, you include the hostname and port: *http://hostname:port*. Or, if you use AEM as a Cloud Service, you can use the author URL: *https://author-xxxxxx-xxxxxxx.adobeaemcloud.com*.

Configuration	Description
`authType`	The type of authentication you use, whether `Basic` or `OAuth2`.
`deploymentType`	The type of Adobe Experience Manager that you use, either `CLOUD` or `ON-PREMISE` .
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.
• `page` • `asset`	A list of objects that map the attributes or field names of your Adobe Experience Manager pages and assets to Amazon Q index field names.
`additionalProperties`	Additional configuration options for your content in your data source.
`isCrawlAcl`	Specify `true` to crawl access control informati on from documents. **Note** Amazon Q Business crawls ACL information to ensure responses are generated only from documents your end users have access to by default. See Authorization for more details.
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.

Configuration	Description
`timeZoneId`	If you use AEM On-Premise and the time zone of your server is different than the time zone of the Amazon Q AEM connector or index, you can specify the server time zone to align with the AEM connector or index. The default time zone for AEM On-Premis e is the time zone of the Amazon Q AEM connector or index. The default time zone for AEM as a Cloud Service is Greenwich Mean Time.
• `pageRootPaths` • `assetRootPaths`	A list of root paths for pages and assets. For example, the root path for a page could be */content/sub* and the root path for an asset could be */content/sub/asset1*.
`crawlAssets`	Specify `true` to crawl assets.
`crawlPages`	Specify `true` to crawl pages.
• `pagePathInclusionPatterns` • `pageNameInclusionPatterns` • `assetPathInclusionPatterns` • `assetTypeInclusionPatterns` • `assetNameInclusionPatterns`	A list of regular expression patterns to include certain pages and assets in your Adobe Experience Manager data source. Pages and assets that match the patterns are included in the index. Pages and assets that don't match the patterns are excluded from the index. If a page or asset matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.

Configuration	Description
• pagePathExclusionPatterns • pageNameExclusionPatterns • assetPathExclusionPatterns • assetTypeInclusionPatterns • assetNameInclusionPatterns	A list of regular expression patterns to exclude certain pages and assets in your Adobe Experience Manager data source. Pages and assets that match the patterns are excluded from the index. Pages and assets that don't match the patterns are included in the index. If a page or asset matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.
pageComponents	A list of names for the specific page components that you want to index.
contentFragmentVariations	A list of names for the specific saved variation s of Adobe Experience Manager Content Fragments that you want to index.
maxFileSizeInMegaBytes	Specify the Maximum file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
type	The type of data source. Specify AEM as your data source type.

Configuration	Description
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/principal informati on on users and groups with access to specific documents. **Note** Amazon Q Business crawls identity information from your data source to ensure responses are generated only from documents end users have access to by default. For more information, see Identity crawler.
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.

Configuration	Description

secretArn	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Adobe Experience Manager. The secret must contain a JSON structure with the following keys:
	
	If using basic authentication for either AEM On-Premise or Cloud:
	
	{
	"aemUrl": "*Adobe Experience Manager On-Premise host URL* ",
	"username": " *username with admin permissions* ",
	"password": " *password with admin permissions* "
	}
	
	If using OAuth 2.0 authentication for AEM On-Premise:
	
	{
	"aemUrl": "*Adobe Experience Manager host URL*",
	"clientId": " *client ID*",
	"clientSecret": " *client secret*",
	"privateKey": " *private key*"
	}
	
	If using OAuth 2.0 authentication for AEM as a Cloud Service:
	
	{
	"clientId": " *client ID*",
	"clientSecret": " *client secret*",
	"privateKey": " *private key*",
	"orgId": "*organization ID* ",

Configuration	Description
	"technicalAccountId": " *technical account ID*", "imsHost": " *Adobe Identity Management System (IMS) host* " }
`version`	The version of this template that's currently supported.

How Amazon Q Business connector crawls AEM (Cloud) ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an AEM (Cloud) data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your AEM (Cloud) instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

The group and user IDs are mapped as follows:

- `_group_ids` – Group IDs exist in Adobe Experience Manager content where there are set access permissions. They're mapped from the names of the groups in AEM.
- `_user_id` – User IDs exist in Adobe Experience Manager content where there are set access permissions. They're mapped from the user emails as the IDs in AEM.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Amazon Q Business AEM (Cloud) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application environment and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Adobe Experience Manager (AEM) connector supports the following entities and the associated reserved and custom attributes.

> **Important**
>
> If you map any AEM (Cloud) field to Amazon Q document title and document body fields, Amazon Q will generate responses from data in the document title and body.

Supported entities and field mappings

- Pages

- Assets

Pages

Amazon Q supports crawling AEM Pages and offers the following page field mappings.

Adobe Experience Manager (AEM) field name	Index field name	Description	Data type
aem_page_source_uri	_source_uri	Default	String
aem_page_createdBy	_authors	Default	String list
aem_page_template	aem_page_template	Custom	String
aem_entity_type	_category	Default	String
aem_page_createdAt	_created_at	Default	Date
aem_page_lastModified	_last_updated_at	Default	Date
aem_page_lastReplicatedBy	aem_page_publisher	Custom	String
aem_page_lastReplicatedAt	aem_page_publishedAt	Custom	Date

Assets

Amazon Q supports crawling AEM Assets and offers the following asset field mappings.

Adobe Experience Manager (AEM) field name	Index field name	Description	Data type
aem_page_source_uri	_source_uri	Default	String

Adobe Experience Manager (AEM) field name	Index field name	Description	Data type
aem_page_createdBy	_authors	Default	String list
aem_entity_type	_category	Default	String
aem_page_createdAt	_created_at	Default	Date
aem_page_lastModified	_last_updated_at	Default	Date
aem_page_lastReplicatedBy	aem_page_publisher	Custom	String
aem_page_lastReplicatedAt	aem_page_publishedAt	Custom	Date

IAM role for Amazon Q AEM (Cloud) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.

- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
```

```
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
```

```
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the AEM (Cloud) connector

The following table provides information about error codes you may see for the AEM (Cloud) connector and suggested resolutions.

Error code	Error message	Suggested resolution
AEM-5001	Error while getting Administrators group. Below are the possible reasons for this error: Provided AEM host URL might be wrong. Provided username and password are invalid or user is non-admin user.	Check whether provided username and password are correct or not. Also ensure that the provided user is either admin or belongs to administrators' group.
AEM-5002	Error while generating OAuth2 access token.	Provide valid OAuth2 credentials.
AEM-5103	Null/empty AEM host URL.	AEM host URL should not be null or empty.
AEM-5104	Error while parsing https response. Below are the possible reasons for this error. 1. Provided AEM host URL might be wrong, please cross-check the AEM host URL. 2. AEM server is down or not reachable.	Provide a valid host URL, or try again later.
AEM-5105	Provided authType is incorrect.	Auth type should be Basic or OAuth2.
AEM-5106	Null/empty AEM username.	Username should not be null or empty value.

Error code	Error message	Suggested resolution
AEM-5107	Null/empty AEM password.	Password should not be null or empty value.
AEM-5108	Null/empty client id.	Client Id should not be null or empty value.
AEM-5109	Null/empty client secret.	Client Secret should not be null or empty value.
AEM-5110	Null/empty private key.	Private key should not be null or empty value.
AEM-5111	Null/empty Page Index field name.	Page index field should not be null or empty value
AEM-5112	Null/empty Page data source field name.	Page data source field should not be null or empty value.
AEM-5113	Null/empty asset Index field name.	Asset index field should not be null or empty value.
AEM-5114	Null/empty asset data source field name.	Asset data source field should not be null or empty value.
AEM-5115	Null/empty crawl type.	crawl Type value should be FULL_CRAWL/CHANG_LOG type.
AEM-5116	Invalid AEM host URL format.	Check whether provided AEM URL is in correct format or not e.g. http<s>://<aem-host>:<port>
AEM-5117	Page root paths are incorrect.	Page root paths must be a list of strings.
AEM-5118	Asset root paths are incorrect.	Asset root paths must be a list of strings.

Error code	Error message	Suggested resolution
AEM-5119	Page path inclusion or exclusion patterns are incorrect.	Page name inclusion patterns/ Exclusion must be a list of strings.
AEM-5120	Asset path inclusion or exclusion patterns are incorrect.	Asset name inclusion patterns/ Exclusion must be a list of strings.
AEM-5121	Provided deploymentype is incorrect.	Deployment type should be either CLOUD or ON_PREMISE.
AEM-5122	Provided orgId is incorrect.	OrgId should not be null or empty value.
AEM-5123	Provided technical Account Id is incorrect.	Technical Account Id should not be null or empty value.
AEM-5124	Provided imsHost is incorrect.	IMS Host should not be null or empty value.
AEM-5125	Null/Empty deployment type.	Deployment type should be either CLOUD or ON_PREMISE.
AEM-5126	Invalid Timezone Id.	Provide a valid timezone id.
AEM-5127	Null/empty asset Index field type.	Asset index field should not be null or empty value.
AEM-5128	Null/empty page Index field type.	Page index field should not be null or empty value.
AEM-5129	DataSourceFieldNam e doesn't match with IndexFieldType.	Provide a valid asset indexFieldType for the provided asset dataSourc eFieldName. Or, provide a valid page indexFieldType for the provided page dataSourceFieldName.

Error code	Error message	Suggested resolution
AEM-5130	Protocol used by provided AEM URL is not supported by AEM connector.	Only https protocol is supported by AEM connector. Provide an AEM URL based on https protocol.
AEM-5131	AEM password is too large.	Password should not be greater than 40 characters.
AEM-5132	AEM client ID is too large.	Client ID should not be greater than 40 characters.
AEM-5133	AEM client secret is too large.	Client secret should not be greater than 40 characters.
AEM-5134	AEM private key is too large.	Private key should not be greater than 2048 characters.
AEM-5135	AEM client ID contains invalid characters.	Client ID should not contain unprintable characters.
AEM-5136	AEM client secret contains invalid characters.	Client secret should not contain unprintable characters.
AEM-5137	AEM private key contains invalid characters.	Private key should not contain unprintable characters.
AEM-5138	AEM IMS host is too large.	IMS host should not be greater than 100 characters.
AEM-5139	AEM technical account ID is too large.	Technical account id should not be greater than 100 characters.
AEM-5140	AEM org ID is too large.	Org id should not be greater than 100 characters.

Error code	Error message	Suggested resolution
AEM-5141	Page name inclusion or exclusion patterns are incorrect.	Page name inclusion patterns/ Exclusion must be a list of strings.
AEM-5142	Asset name inclusion or exclusion patterns are incorrect.	Asset name inclusion patterns/ Exclusion must be a list of strings.
AEM-5143	Asset type inclusion or exclusion patterns are incorrect.	Asset type inclusion patterns/Exclusion must be a list of strings.
AEM-5144	Invalid page root path. Please provide valid page root path.	Page path should start with /content.
AEM-5145	Invalid asset root path. Please provide valid asset root path.	Asset path should start with /content/ dam.
AEM-5146	AEM page root paths list size is too large.	Page root paths list size should not be greater than 1000.
AEM-5147	AEM asset root paths list size is too large.	Asset root paths list size should not be greater than 1000.
AEM-5148	Asset root paths list size should not be greater than 1000.	Asset path exclusion patterns list size should not be greater than 1000.
AEM-5149	AEM asset path inclusion pattern list size is too large.	Asset path inclusion patterns list size should not be greater than 1000.
AEM-5150	AEM asset name inclusion pattern list size is too large.	Asset name inclusion patterns list size should not be greater than 1000.

Error code	Error message	Suggested resolution
AEM-5151	AEM asset name exclusion pattern list size is too large.	Asset name exclusion patterns list size should not be greater than 1000.
AEM-5152	AEM asset type exclusion pattern list size is too large.	Asset type exclusion patterns list size should not be greater than 1000.
AEM-5153	AEM asset type inclusion pattern list size is too large.	Asset type inclusion patterns list size should not be greater than 1000.
AEM-5154	AEM page name inclusion pattern list size is too large.	Page name inclusion patterns list size should not be greater than 1000.
AEM-5155	AEM page name Exclusion pattern list size is too large.	Page name exclusion patterns list size should not be greater than 1000.
AEM-5156	AEM page path Exclusion pattern list size is too large.	Page path exclusion patterns list size should not be greater than 1000.
AEM-5157	AEM page path inclusion pattern list size is too large.	Page path inclusion patterns list size should not be greater than 1000.
AEM-5158	AEM page components list size is too large.	Page components list size should not be greater than 1000.
AEM-5159	AEM content fragment variations list size is too large.	Content fragment variations list size should not be greater than 1000.
AEM-5160	AEM host URL characters length is too large.	AEM host URL characters length should not be greater than 2048 characters.

Error code	Error message	Suggested resolution
AEM-5161	Some of the page root paths exceed the character limit.	Page root path characters length should not be greater than 1000.
AEM-5162	Some of the asset root paths exceed the character limit.	Asset root Path characters length should not be greater than 1000 .
AEM-5163	Some of the asset path exclusion objects exceed the character limit.	Asset path exclusion characters length should not be greater than 1000.
AEM-5164	Some of the asset path inclusion objects exceed the character limit.	Asset path inclusion characters length should not be greater than 1000.
AEM-5165	Some of the asset name inclusion objects exceed the character limit.	Asset name inclusion characters length should not be greater than 1000.
AEM-5166	Some of the asset name exclusion objects exceed the character limit.	Asset name exclusion characters length should not be greater than 1000.
AEM-5167	Some of the asset type exclusion objects exceed the character limit.	Asset type exclusion characters length should not be greater than 1000.
AEM-5168	Some of the asset type inclusion objects exceed the character limit.	Asset type inclusion characters length should not be greater than 1000.
AEM-5169	Some of the page name inclusion objects exceed the character limit.	Page name inclusion characters length should not be greater than 1000.

Error code	Error message	Suggested resolution
AEM-5170	Some of the page name exclusion objects exceed the character limit.	Page name exclusion characters length should not be greater than 1000.
AEM-5171	Some of the page path exclusion objects exceed the character limit.	Page path exclusion characters length should not be greater than 1000.
AEM-5172	Some of the page path inclusion objects exceed the character limit.	Page path inclusion characters length should not be greater than 1000.
AEM-5300	Error in serializing change log token.	Retry sync.
AEM-5301	Error in de-serializing change log token.	Retry sync.
AEM-5401	Error occurred while getting AEM groups.	Retry sync.
AEM-5501	Could not connect to host.	
AEM-5502	AEM URL SSRF check failed.	Make sure AEM host URL is not a multicast/local/link-local/loopback address.
AEM-5503	AEM host not found.	Check whether AEM host is up and reachable.
AEM-5504	Error occurred while executing HTTP request against given AEM URL.	Check whether AEM host is up and reachable.
AEM-5505	AEM malformed URL error.	Provide valid AEM url.

Error code	Error message	Suggested resolution
AEM-5506	AEM VPC Configuration check failed.	Site local address is restricted.
AEM-5507	Error in creating document attribute.	Only String, String List, Date and Long formats are supported for field mappings.
AEM-5200	Error occurred while getting pages from AEM for Full Crawl.	Check whether AEM server is up and responding to API requests.
AEM-5506	AEM VPC Configuration check failed.	Site local address is restricted.
AEM-5201	Error occurred while getting assets from AEM for Full Crawl.	Check whether AEM server is up and responding to API requests.
AEM-5303	Error occurred while getting pages from AEM for Change Log.	Check whether AEM server is up and responding to API requests.
AEM-5304	Error occurred while getting assets from AEM for Change Log.	Check whether AEM server is up and responding to API requests.

Connecting AEM (Server) to Amazon Q Business

Note

AEM (Server) connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend

exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Adobe Experience Manager (AEM) is a content management system (CMS) that's used for creating website or mobile app content. You can connect AEM (Server) instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the AEM (Server) connector
- AEM (Server) connector overview
- Prerequisites for connecting Amazon Q Business to AEM (Server)
- Connecting Amazon Q Business to AEM (Server) using the console
- Connecting Amazon Q Business to AEM (Server) using APIs
- How Amazon Q Business connector crawls AEM (Server) ACLs
- AEM (Server) data source connector field mappings
- IAM role for AEM (Server) connector
- Understand error codes in the AEM (Server) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the AEM (Server) connector

The AEM (Server) connector has the following known limitations:

- Deleted site pages can't be tracked when you use **Change log** sync or **Sync only new, modified, or deleted document sync**.

AEM (Server) connector overview

The following table gives an overview of the Amazon Q Business AEM (Server) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic, OAuth 2.0 with Client Credentials Flow
	Authentication credentials	**Basic** • AEM (Server) host URL • Username of AEM user • Password of AEM user **OAuth 2.0 with Client Credentials Flow** • AEM (Server) host URL • Client ID • Client secret • Private key **Important** Admin privileges required.
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes

Category	Feature	Support
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Pages • Assets See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include/exclude by asset name • Include/exclude by asset type • Include/exclude by asset path • Include/exclude by page name • Include/exclude by page path
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to AEM (Server)

Before you begin, make sure that you have completed the following prerequisites.

In AEM, make sure you have:

- Access to an account with administrative permissions, or an admin user.
- Copied your AEM host URL.
- Noted your basic authentication credentials of admin username and password.

- (Optional) Added the following OAuth scopes if you're using OAuth 2.0 authentication:
  - **Profile** – Needed to get user and groups related data, like email ID and username.
  - **Replicate** – Needed to get data and metadata from Assets and Pages (not including user data).
- **Optional**: Generated OAuth 2.0 credentials in AEM On-Premise. If you use AEM On-Premise, the credentials include client ID, client secret, and private key. Adobe Granite OAuth 2.0 server implementation (com.adobe.granite.oauth.server) provides the support for OAuth 2.0 server functionalities in AEM.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your AEM (Server) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to AEM (Server) using the console

The following procedure outlines how to connect Amazon Q Business to AEM (Server) using the AWS Management Console.

Connecting Amazon Q to AEM (Server)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.

4. Then, on the **Add data sources** page, from **Data sources**, add the **Adobe Experience Manager** data source to your Amazon Q application.
5. Then, on the **AEM (Server)** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. **Source** – Choose **AEM (Server)** .

   a. **AEM host URL** – Enter your **AEM host URL**. If you use AEM On-Premise, you include the hostname and port. For example: `https://hostname:port`.

   b. **SSL certificate location** – Enter the path to the SSL certificate stored in an Amazon S3 bucket. You use this to connect to AEM On-Premise with a secure SSL connection.
8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
9. **Authentication** – Choose between **Basic authentication** and **OAuth 2.0 authentication** and then enter the following information for your **AWS Secrets Manager secret**.

   a. **Basic authentication** – Enter the name for your secret, your AEM site admin username, and admin password.

   b. **OAuth 2.0 authentication** – Enter enter a name for the secret, your client ID, client secret, and private key.
10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

For more information, see VPC.

11. **Identity crawler** – Amazon Q crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.
12. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

13. In **Sync scope**, enter the following information:

a. **Sync content types** – Choose whether to crawl only **Pages** or **Assets**, or both.

b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

c. **Additional configuration – *optional*** – Configure the following settings:

- **Page components** – The specific names of page components. The Page Component is an extensible page component designed to work with the Adobe AEM template editor and allows page header and footer and structure components to be assembled with the template editor.
- **Content fragment variations** – The specific names of content fragment variations. Content Fragments allow you to design, create, curate and publish page-independent content in Adobe AEM. They allow you to prepare content ready for use in multiple locations and over multiple channels.
- **Root paths** – The root paths to specific content.

- **Regex patterns** – The regular expression patterns to include or exclude certain pages and assets.

d. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

- **Full sync** – Sync all content regardless of the previous sync status.
- **New or modified content sync** – Sync only new and modified documents.
- **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

For more details, see Sync mode.

15. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
16. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
17. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

18. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to AEM (Server) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

AEM JSON schema

The following is the AEM JSON schema:

```
{
```

```
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "aemUrl": {
              "type": "string",
              "pattern": "https:.*"
            },
            "authType": {
              "type": "string",
              "enum": [
                "Basic",
                "OAuth2"
              ]
            },
            "deploymentType": {
              "type": "string",
              "enum": [
                "CLOUD",
                "ON_PREMISE"
              ]
            }
          },
          "required": [
            "aemUrl",
            "authType",
            "deploymentType"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "page": {
          "type": "object",
```

```
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": [
                        "STRING",
                        "STRING_LIST",
                        "DATE",
                        "LONG"
                      ]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": [
            "fieldMappings"
          ]
        },
        "asset": {
          "type": "object",
          "properties": {
            "fieldMappings": {
```

```
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "STRING_LIST",
                      "DATE",
                      "LONG"
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "isCrawlAcl": {
```

```
          "type": "boolean"
        },
        "fieldForUserId": {
          "type": "string"
        },
        "timeZoneId": {
          "type": "string",
          "enum": [
            "Africa/Abidjan",
            "Africa/Accra",
            "Africa/Addis_Ababa",
            "Africa/Algiers",
            "Africa/Asmara",
            "Africa/Asmera",
            "Africa/Bamako",
            "Africa/Bangui",
            "Africa/Banjul",
            "Africa/Bissau",
            "Africa/Blantyre",
            "Africa/Brazzaville",
            "Africa/Bujumbura",
            "Africa/Cairo",
            "Africa/Casablanca",
            "Africa/Ceuta",
            "Africa/Conakry",
            "Africa/Dakar",
            "Africa/Dar_es_Salaam",
            "Africa/Djibouti",
            "Africa/Douala",
            "Africa/El_Aaiun",
            "Africa/Freetown",
            "Africa/Gaborone",
            "Africa/Harare",
            "Africa/Johannesburg",
            "Africa/Juba",
            "Africa/Kampala",
            "Africa/Khartoum",
            "Africa/Kigali",
            "Africa/Kinshasa",
            "Africa/Lagos",
            "Africa/Libreville",
            "Africa/Lome",
            "Africa/Luanda",
            "Africa/Lubumbashi",
```

```
            "Africa/Lusaka",
            "Africa/Malabo",
            "Africa/Maputo",
            "Africa/Maseru",
            "Africa/Mbabane",
            "Africa/Mogadishu",
            "Africa/Monrovia",
            "Africa/Nairobi",
            "Africa/Ndjamena",
            "Africa/Niamey",
            "Africa/Nouakchott",
            "Africa/Ouagadougou",
            "Africa/Porto-Novo",
            "Africa/Sao_Tome",
            "Africa/Timbuktu",
            "Africa/Tripoli",
            "Africa/Tunis",
            "Africa/Windhoek",
            "America/Adak",
            "America/Anchorage",
            "America/Anguilla",
            "America/Antigua",
            "America/Araguaina",
            "America/Argentina/Buenos_Aires",
            "America/Argentina/Catamarca",
            "America/Argentina/ComodRivadavia",
            "America/Argentina/Cordoba",
            "America/Argentina/Jujuy",
            "America/Argentina/La_Rioja",
            "America/Argentina/Mendoza",
            "America/Argentina/Rio_Gallegos",
            "America/Argentina/Salta",
            "America/Argentina/San_Juan",
            "America/Argentina/San_Luis",
            "America/Argentina/Tucuman",
            "America/Argentina/Ushuaia",
            "America/Aruba",
            "America/Asuncion",
            "America/Atikokan",
            "America/Atka",
            "America/Bahia",
            "America/Bahia_Banderas",
            "America/Barbados",
            "America/Belem",
```

```
            "America/Belize",
            "America/Blanc-Sablon",
            "America/Boa_Vista",
            "America/Bogota",
            "America/Boise",
            "America/Buenos_Aires",
            "America/Cambridge_Bay",
            "America/Campo_Grande",
            "America/Cancun",
            "America/Caracas",
            "America/Catamarca",
            "America/Cayenne",
            "America/Cayman",
            "America/Chicago",
            "America/Chihuahua",
            "America/Ciudad_Juarez",
            "America/Coral_Harbour",
            "America/Cordoba",
            "America/Costa_Rica",
            "America/Creston",
            "America/Cuiaba",
            "America/Curacao",
            "America/Danmarkshavn",
            "America/Dawson",
            "America/Dawson_Creek",
            "America/Denver",
            "America/Detroit",
            "America/Dominica",
            "America/Edmonton",
            "America/Eirunepe",
            "America/El_Salvador",
            "America/Ensenada",
            "America/Fort_Nelson",
            "America/Fort_Wayne",
            "America/Fortaleza",
            "America/Glace_Bay",
            "America/Godthab",
            "America/Goose_Bay",
            "America/Grand_Turk",
            "America/Grenada",
            "America/Guadeloupe",
            "America/Guatemala",
            "America/Guayaquil",
            "America/Guyana",
```

```
            "America/Halifax",
            "America/Havana",
            "America/Hermosillo",
            "America/Indiana/Indianapolis",
            "America/Indiana/Knox",
            "America/Indiana/Marengo",
            "America/Indiana/Petersburg",
            "America/Indiana/Tell_City",
            "America/Indiana/Vevay",
            "America/Indiana/Vincennes",
            "America/Indiana/Winamac",
            "America/Indianapolis",
            "America/Inuvik",
            "America/Iqaluit",
            "America/Jamaica",
            "America/Jujuy",
            "America/Juneau",
            "America/Kentucky/Louisville",
            "America/Kentucky/Monticello",
            "America/Knox_IN",
            "America/Kralendijk",
            "America/La_Paz",
            "America/Lima",
            "America/Los_Angeles",
            "America/Louisville",
            "America/Lower_Princes",
            "America/Maceio",
            "America/Managua",
            "America/Manaus",
            "America/Marigot",
            "America/Martinique",
            "America/Matamoros",
            "America/Mazatlan",
            "America/Mendoza",
            "America/Menominee",
            "America/Merida",
            "America/Metlakatla",
            "America/Mexico_City",
            "America/Miquelon",
            "America/Moncton",
            "America/Monterrey",
            "America/Montevideo",
            "America/Montreal",
            "America/Montserrat",
```

```
            "America/Nassau",
            "America/New_York",
            "America/Nipigon",
            "America/Nome",
            "America/Noronha",
            "America/North_Dakota/Beulah",
            "America/North_Dakota/Center",
            "America/North_Dakota/New_Salem",
            "America/Nuuk",
            "America/Ojinaga",
            "America/Panama",
            "America/Pangnirtung",
            "America/Paramaribo",
            "America/Phoenix",
            "America/Port-au-Prince",
            "America/Port_of_Spain",
            "America/Porto_Acre",
            "America/Porto_Velho",
            "America/Puerto_Rico",
            "America/Punta_Arenas",
            "America/Rainy_River",
            "America/Rankin_Inlet",
            "America/Recife",
            "America/Regina",
            "America/Resolute",
            "America/Rio_Branco",
            "America/Rosario",
            "America/Santa_Isabel",
            "America/Santarem",
            "America/Santiago",
            "America/Santo_Domingo",
            "America/Sao_Paulo",
            "America/Scoresbysund",
            "America/Shiprock",
            "America/Sitka",
            "America/St_Barthelemy",
            "America/St_Johns",
            "America/St_Kitts",
            "America/St_Lucia",
            "America/St_Thomas",
            "America/St_Vincent",
            "America/Swift_Current",
            "America/Tegucigalpa",
            "America/Thule",
```

```
            "America/Thunder_Bay",
            "America/Tijuana",
            "America/Toronto",
            "America/Tortola",
            "America/Vancouver",
            "America/Virgin",
            "America/Whitehorse",
            "America/Winnipeg",
            "America/Yakutat",
            "America/Yellowknife",
            "Antarctica/Casey",
            "Antarctica/Davis",
            "Antarctica/DumontDUrville",
            "Antarctica/Macquarie",
            "Antarctica/Mawson",
            "Antarctica/McMurdo",
            "Antarctica/Palmer",
            "Antarctica/Rothera",
            "Antarctica/South_Pole",
            "Antarctica/Syowa",
            "Antarctica/Troll",
            "Antarctica/Vostok",
            "Arctic/Longyearbyen",
            "Asia/Aden",
            "Asia/Almaty",
            "Asia/Amman",
            "Asia/Anadyr",
            "Asia/Aqtau",
            "Asia/Aqtobe",
            "Asia/Ashgabat",
            "Asia/Ashkhabad",
            "Asia/Atyrau",
            "Asia/Baghdad",
            "Asia/Bahrain",
            "Asia/Baku",
            "Asia/Bangkok",
            "Asia/Barnaul",
            "Asia/Beirut",
            "Asia/Bishkek",
            "Asia/Brunei",
            "Asia/Calcutta",
            "Asia/Chita",
            "Asia/Choibalsan",
            "Asia/Chongqing",
```

```
            "Asia/Chungking",
            "Asia/Colombo",
            "Asia/Dacca",
            "Asia/Damascus",
            "Asia/Dhaka",
            "Asia/Dili",
            "Asia/Dubai",
            "Asia/Dushanbe",
            "Asia/Famagusta",
            "Asia/Gaza",
            "Asia/Harbin",
            "Asia/Hebron",
            "Asia/Ho_Chi_Minh",
            "Asia/Hong_Kong",
            "Asia/Hovd",
            "Asia/Irkutsk",
            "Asia/Istanbul",
            "Asia/Jakarta",
            "Asia/Jayapura",
            "Asia/Jerusalem",
            "Asia/Kabul",
            "Asia/Kamchatka",
            "Asia/Karachi",
            "Asia/Kashgar",
            "Asia/Kathmandu",
            "Asia/Katmandu",
            "Asia/Khandyga",
            "Asia/Kolkata",
            "Asia/Krasnoyarsk",
            "Asia/Kuala_Lumpur",
            "Asia/Kuching",
            "Asia/Kuwait",
            "Asia/Macao",
            "Asia/Macau",
            "Asia/Magadan",
            "Asia/Makassar",
            "Asia/Manila",
            "Asia/Muscat",
            "Asia/Nicosia",
            "Asia/Novokuznetsk",
            "Asia/Novosibirsk",
            "Asia/Omsk",
            "Asia/Oral",
            "Asia/Phnom_Penh",
```

```
            "Asia/Pontianak",
            "Asia/Pyongyang",
            "Asia/Qatar",
            "Asia/Qostanay",
            "Asia/Qyzylorda",
            "Asia/Rangoon",
            "Asia/Riyadh",
            "Asia/Saigon",
            "Asia/Sakhalin",
            "Asia/Samarkand",
            "Asia/Seoul",
            "Asia/Shanghai",
            "Asia/Singapore",
            "Asia/Srednekolymsk",
            "Asia/Taipei",
            "Asia/Tashkent",
            "Asia/Tbilisi",
            "Asia/Tehran",
            "Asia/Tel_Aviv",
            "Asia/Thimbu",
            "Asia/Thimphu",
            "Asia/Tokyo",
            "Asia/Tomsk",
            "Asia/Ujung_Pandang",
            "Asia/Ulaanbaatar",
            "Asia/Ulan_Bator",
            "Asia/Urumqi",
            "Asia/Ust-Nera",
            "Asia/Vientiane",
            "Asia/Vladivostok",
            "Asia/Yakutsk",
            "Asia/Yangon",
            "Asia/Yekaterinburg",
            "Asia/Yerevan",
            "Atlantic/Azores",
            "Atlantic/Bermuda",
            "Atlantic/Canary",
            "Atlantic/Cape_Verde",
            "Atlantic/Faeroe",
            "Atlantic/Faroe",
            "Atlantic/Jan_Mayen",
            "Atlantic/Madeira",
            "Atlantic/Reykjavik",
            "Atlantic/South_Georgia",
```

```
            "Atlantic/St_Helena",
            "Atlantic/Stanley",
            "Australia/ACT",
            "Australia/Adelaide",
            "Australia/Brisbane",
            "Australia/Broken_Hill",
            "Australia/Canberra",
            "Australia/Currie",
            "Australia/Darwin",
            "Australia/Eucla",
            "Australia/Hobart",
            "Australia/LHI",
            "Australia/Lindeman",
            "Australia/Lord_Howe",
            "Australia/Melbourne",
            "Australia/NSW",
            "Australia/North",
            "Australia/Perth",
            "Australia/Queensland",
            "Australia/South",
            "Australia/Sydney",
            "Australia/Tasmania",
            "Australia/Victoria",
            "Australia/West",
            "Australia/Yancowinna",
            "Brazil/Acre",
            "Brazil/DeNoronha",
            "Brazil/East",
            "Brazil/West",
            "CET",
            "CST6CDT",
            "Canada/Atlantic",
            "Canada/Central",
            "Canada/Eastern",
            "Canada/Mountain",
            "Canada/Newfoundland",
            "Canada/Pacific",
            "Canada/Saskatchewan",
            "Canada/Yukon",
            "Chile/Continental",
            "Chile/EasterIsland",
            "Cuba",
            "EET",
            "EST5EDT",
```

```
            "Egypt",
            "Eire",
            "Etc/GMT",
            "Etc/GMT+0",
            "Etc/GMT+1",
            "Etc/GMT+10",
            "Etc/GMT+11",
            "Etc/GMT+12",
            "Etc/GMT+2",
            "Etc/GMT+3",
            "Etc/GMT+4",
            "Etc/GMT+5",
            "Etc/GMT+6",
            "Etc/GMT+7",
            "Etc/GMT+8",
            "Etc/GMT+9",
            "Etc/GMT-0",
            "Etc/GMT-1",
            "Etc/GMT-10",
            "Etc/GMT-11",
            "Etc/GMT-12",
            "Etc/GMT-13",
            "Etc/GMT-14",
            "Etc/GMT-2",
            "Etc/GMT-3",
            "Etc/GMT-4",
            "Etc/GMT-5",
            "Etc/GMT-6",
            "Etc/GMT-7",
            "Etc/GMT-8",
            "Etc/GMT-9",
            "Etc/GMT0",
            "Etc/Greenwich",
            "Etc/UCT",
            "Etc/UTC",
            "Etc/Universal",
            "Etc/Zulu",
            "Europe/Amsterdam",
            "Europe/Andorra",
            "Europe/Astrakhan",
            "Europe/Athens",
            "Europe/Belfast",
            "Europe/Belgrade",
            "Europe/Berlin",
```

```
            "Europe/Bratislava",
            "Europe/Brussels",
            "Europe/Bucharest",
            "Europe/Budapest",
            "Europe/Busingen",
            "Europe/Chisinau",
            "Europe/Copenhagen",
            "Europe/Dublin",
            "Europe/Gibraltar",
            "Europe/Guernsey",
            "Europe/Helsinki",
            "Europe/Isle_of_Man",
            "Europe/Istanbul",
            "Europe/Jersey",
            "Europe/Kaliningrad",
            "Europe/Kiev",
            "Europe/Kirov",
            "Europe/Kyiv",
            "Europe/Lisbon",
            "Europe/Ljubljana",
            "Europe/London",
            "Europe/Luxembourg",
            "Europe/Madrid",
            "Europe/Malta",
            "Europe/Mariehamn",
            "Europe/Minsk",
            "Europe/Monaco",
            "Europe/Moscow",
            "Europe/Nicosia",
            "Europe/Oslo",
            "Europe/Paris",
            "Europe/Podgorica",
            "Europe/Prague",
            "Europe/Riga",
            "Europe/Rome",
            "Europe/Samara",
            "Europe/San_Marino",
            "Europe/Sarajevo",
            "Europe/Saratov",
            "Europe/Simferopol",
            "Europe/Skopje",
            "Europe/Sofia",
            "Europe/Stockholm",
            "Europe/Tallinn",
```

```
            "Europe/Tirane",
            "Europe/Tiraspol",
            "Europe/Ulyanovsk",
            "Europe/Uzhgorod",
            "Europe/Vaduz",
            "Europe/Vatican",
            "Europe/Vienna",
            "Europe/Vilnius",
            "Europe/Volgograd",
            "Europe/Warsaw",
            "Europe/Zagreb",
            "Europe/Zaporozhye",
            "Europe/Zurich",
            "GB",
            "GB-Eire",
            "GMT",
            "GMT0",
            "Greenwich",
            "Hongkong",
            "Iceland",
            "Indian/Antananarivo",
            "Indian/Chagos",
            "Indian/Christmas",
            "Indian/Cocos",
            "Indian/Comoro",
            "Indian/Kerguelen",
            "Indian/Mahe",
            "Indian/Maldives",
            "Indian/Mauritius",
            "Indian/Mayotte",
            "Indian/Reunion",
            "Iran",
            "Israel",
            "Jamaica",
            "Japan",
            "Kwajalein",
            "Libya",
            "MET",
            "MST7MDT",
            "Mexico/BajaNorte",
            "Mexico/BajaSur",
            "Mexico/General",
            "NZ",
            "NZ-CHAT",
```

```
            "Navajo",
            "PRC",
            "PST8PDT",
            "Pacific/Apia",
            "Pacific/Auckland",
            "Pacific/Bougainville",
            "Pacific/Chatham",
            "Pacific/Chuuk",
            "Pacific/Easter",
            "Pacific/Efate",
            "Pacific/Enderbury",
            "Pacific/Fakaofo",
            "Pacific/Fiji",
            "Pacific/Funafuti",
            "Pacific/Galapagos",
            "Pacific/Gambier",
            "Pacific/Guadalcanal",
            "Pacific/Guam",
            "Pacific/Honolulu",
            "Pacific/Johnston",
            "Pacific/Kanton",
            "Pacific/Kiritimati",
            "Pacific/Kosrae",
            "Pacific/Kwajalein",
            "Pacific/Majuro",
            "Pacific/Marquesas",
            "Pacific/Midway",
            "Pacific/Nauru",
            "Pacific/Niue",
            "Pacific/Norfolk",
            "Pacific/Noumea",
            "Pacific/Pago_Pago",
            "Pacific/Palau",
            "Pacific/Pitcairn",
            "Pacific/Pohnpei",
            "Pacific/Ponape",
            "Pacific/Port_Moresby",
            "Pacific/Rarotonga",
            "Pacific/Saipan",
            "Pacific/Samoa",
            "Pacific/Tahiti",
            "Pacific/Tarawa",
            "Pacific/Tongatapu",
            "Pacific/Truk",
```

```
            "Pacific/Wake",
            "Pacific/Wallis",
            "Pacific/Yap",
            "Poland",
            "Portugal",
            "ROK",
            "Singapore",
            "SystemV/AST4",
            "SystemV/AST4ADT",
            "SystemV/CST6",
            "SystemV/CST6CDT",
            "SystemV/EST5",
            "SystemV/EST5EDT",
            "SystemV/HST10",
            "SystemV/MST7",
            "SystemV/MST7MDT",
            "SystemV/PST8",
            "SystemV/PST8PDT",
            "SystemV/YST9",
            "SystemV/YST9YDT",
            "Turkey",
            "UCT",
            "US/Alaska",
            "US/Aleutian",
            "US/Arizona",
            "US/Central",
            "US/East-Indiana",
            "US/Eastern",
            "US/Hawaii",
            "US/Indiana-Starke",
            "US/Michigan",
            "US/Mountain",
            "US/Pacific",
            "US/Samoa",
            "UTC",
            "Universal",
            "W-SU",
            "WET",
            "Zulu",
            "EST",
            "HST",
            "MST",
            "ACT",
            "AET",
```

```
            "AGT",
            "ART",
            "AST",
            "BET",
            "BST",
            "CAT",
            "CNT",
            "CST",
            "CTT",
            "EAT",
            "ECT",
            "IET",
            "IST",
            "JST",
            "MIT",
            "NET",
            "NST",
            "PLT",
            "PNT",
            "PRT",
            "PST",
            "SST",
            "VST"
          ]
        },
        "pageRootPaths": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "assetRootPaths": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "crawlAssets": {
          "type": "boolean"
        },
        "crawlPages": {
          "type": "boolean"
        },
        "pagePathInclusionPatterns": {
```

```
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "pagePathExclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "pageNameInclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "pageNameExclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "assetPathInclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "assetPathExclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "assetTypeInclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "assetTypeExclusionPatterns": {
          "type": "array",
          "items": {
```

```
            "type": "string"
          }
        },
        "assetNameInclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "assetNameExclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "pageComponents": {
          "type": "array",
          "items": {
            "type": "object"
          }
        },
        "contentFragmentVariations": {
          "type": "array",
          "items": {
            "type": "object"
          }
        },
        "cugExemptedPrincipals": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        }
      },
      "required": []
    },
    "type": {
      "type": "string",
      "pattern": "AEM"
    },
    "enableIdentityCrawler": {
```

```
      "type": "boolean"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the endpoint for the data source.
`repositoryEndpointMetadata`	The endpoint information for the data source.

Configuration	Description
`aemUrl`	The Adobe Experience Manager host URL. For example, if you use AEM On-Premise, you include the hostname and port: *http://hostname:port*. Or, if you use AEM as a Cloud Service, you can use the author URL: *https://author-xxxxxx-xxxxxxx.adobeaemcloud.com*.
`authType`	The type of authentication you use, whether `Basic` or `OAuth2`.
`deploymentType`	The type of Adobe Experience Manager that you use, either `CLOUD` or `ON-PREMISE` .
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.
• `page` • `asset`	A list of objects that map the attributes or field names of your Adobe Experience Manager pages and assets to Amazon Q index field names.
`additionalProperties`	Additional configuration options for your content in your data source.
`isCrawlAcl`	Specify `true` to crawl access control information from documents. **Note** Amazon Q Business crawls ACL information to ensure responses are generated only from documents your end users have access to. See Authorization for more details.

Configuration	Description
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.
`timeZoneId`	If you use AEM On-Premise and the time zone of your server is different than the time zone of the Amazon Q AEM connector or index, you can specify the server time zone to align with the AEM connector or index. The default time zone for AEM On-Premis e is the time zone of the Amazon Q AEM connector or index. The default time zone for AEM as a Cloud Service is Greenwich Mean Time.
• `pageRootPaths` • `assetRootPaths`	A list of root paths for pages and assets. For example, the root path for a page could be */content/sub* and the root path for an asset could be */content/sub/asset1*.
`crawlAssets`	Specify `true` to crawl assets.
`crawlPages`	Specify `true` to crawl pages.
• `pagePathInclusionPatterns` • `pageNameInclusionPatterns` • `assetPathInclusionPatterns` • `assetTypeInclusionPatterns` • `assetNameInclusionPatterns`	A list of regular expression patterns to include certain pages and assets in your Adobe Experience Manager data source. Pages and assets that match the patterns are included in the index. Pages and assets that don't match the patterns are excluded from the index. If a page or asset matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.

Configuration	Description
• pagePathExclusionPatterns • pageNameExclusionPatterns • assetPathExclusionPatterns • assetTypeInclusionPatterns • assetNameInclusionPatterns	A list of regular expression patterns to exclude certain pages and assets in your Adobe Experience Manager data source. Pages and assets that match the patterns are excluded from the index. Pages and assets that don't match the patterns are included in the index. If a page or asset matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.
pageComponents	A list of names for the specific page components that you want to index.
contentFragmentVariations	A list of names for the specific saved variation s of Adobe Experience Manager Content Fragments that you want to index.
maxFileSizeInMegaBytes	Specify the Maximum file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
type	The type of data source. Specify AEM as your data source type.

Configuration	Description
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/principal informati on on users and groups with access to specific documents. **Note** Amazon Q Business crawls identity information from your data source to ensure responses are generated only from documents end users have access to by default. For more information, see Identity crawler.
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.

Configuration	Description

secretArn	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Adobe Experience Manager. The secret must contain a JSON structure with the following keys:
	
	If using basic authentication for either AEM On-Premise or Cloud:
	
	{
	"aemUrl": "*Adobe Experience Manager On-Premise host URL* ",
	"username": " *username with admin permissions* ",
	"password": " *password with admin permissions* "
	}
	
	If using OAuth 2.0 authentication for AEM On-Premise:
	
	{
	"aemUrl": "*Adobe Experience Manager host URL*",
	"clientId": " *client ID*",
	"clientSecret": " *client secret*",
	"privateKey": " *private key*"
	}
	
	If using OAuth 2.0 authentication for AEM as a Cloud Service:
	
	{
	"clientId": " *client ID*",
	"clientSecret": " *client secret*",
	"privateKey": " *private key*",
	"orgId": "*organization ID* ",

Configuration	Description

	<pre>{
	"technicalAccountId": " *technical account ID*",
	"imsHost": " *Adobe Identity Management System (IMS) host* "
	}</pre>

`version`	The version of this template that's currently supported.

How Amazon Q Business connector crawls AEM (Server) ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an AEM (Server) data source to Amazon Q Business, Amazon Q crawls ACL information attached to a document (user and group information) from your AEM (Server) instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

The group and user IDs are mapped as follows:

- `_group_ids` – Group IDs exist in Adobe Experience Manager content where there are set access permissions. They're mapped from the names of the groups in AEM.
- `_user_id` – User IDs exist in Adobe Experience Manager content where there are set access permissions. They're mapped from the user emails as the IDs in AEM.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

AEM (Server) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application environment and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Adobe Experience Manager (AEM) connector supports the following entities and the associated reserved and custom attributes.

> **Important**
>
> If you map any AEM (Server) field to Amazon Q document title and document body fields, Amazon Q will generate responses from data in the document title and body.

Supported entities and field mappings

- Pages

- Assets

Pages

Amazon Q supports crawling AEM Pages and offers the following page field mappings.

Adobe Experience Manager (AEM) field name	Index field name	Description	Data type
aem_page_source_uri	_source_uri	Default	String
aem_page_createdBy	_authors	Default	String list
aem_page_template	aem_page_template	Custom	String
aem_entity_type	_category	Default	String
aem_page_createdAt	_created_at	Default	Date
aem_page_lastModified	_last_updated_at	Default	Date
aem_page_lastReplicatedBy	aem_page_publisher	Custom	String
aem_page_lastReplicatedAt	aem_page_publishedAt	Custom	Date

Assets

Amazon Q supports crawling AEM Assets and offers the following asset field mappings.

Adobe Experience Manager (AEM) field name	Index field name	Description	Data type
aem_page_source_uri	_source_uri	Default	String

Adobe Experience Manager (AEM) field name	Index field name	Description	Data type
aem_page_createdBy	_authors	Default	String list
aem_entity_type	_category	Default	String
aem_page_createdAt	_created_at	Default	Date
aem_page_lastModified	_last_updated_at	Default	Date
aem_page_lastReplicatedBy	aem_page_publisher	Custom	String
aem_page_lastReplicatedAt	aem_page_publishedAt	Custom	Date

IAM role for AEM (Server) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.

- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
```

```
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
```

```
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the AEM (Server) connector

The following table provides information about error codes you may see for the AEM (Server) connector and suggested resolutions.

Error code	Error message	Suggested resolution
AEM-5001	Error while getting Administrators group. Below are the possible reasons for this error: Provided AEM host URL might be wrong. Provided username and password are invalid or user is non-admin user.	Check whether provided username and password are correct or not. Also ensure that the provided user is either admin or belongs to administrators' group.
AEM-5002	Error while generating OAuth2 access token.	Provide valid OAuth2 credentials.
AEM-5103	Null/empty AEM host URL.	AEM host URL should not be null or empty.
AEM-5104	Error while parsing https response. Below are the possible reasons for this error. 1. Provided AEM host URL might be wrong, please cross-check the AEM host URL. 2. AEM server is down or not reachable.	Provide a valid host URL, or try again later.
AEM-5105	Provided authType is incorrect.	Auth type should be Basic or OAuth2.
AEM-5106	Null/empty AEM username.	Username should not be null or empty value.

Error code	Error message	Suggested resolution
AEM-5107	Null/empty AEM password.	Password should not be null or empty value.
AEM-5108	Null/empty client id.	Client Id should not be null or empty value.
AEM-5109	Null/empty client secret.	Client Secret should not be null or empty value.
AEM-5110	Null/empty private key.	Private key should not be null or empty value.
AEM-5111	Null/empty Page Index field name.	Page index field should not be null or empty value
AEM-5112	Null/empty Page data source field name.	Page data source field should not be null or empty value.
AEM-5113	Null/empty asset Index field name.	Asset index field should not be null or empty value.
AEM-5114	Null/empty asset data source field name.	Asset data source field should not be null or empty value.
AEM-5115	Null/empty crawl type.	crawl Type value should be FULL_CRAWL/CHANG_LOG type.
AEM-5116	Invalid AEM host URL format.	Check whether provided AEM URL is in correct format or not e.g. http<s>://<aem-host>:<port>
AEM-5117	Page root paths are incorrect.	Page root paths must be a list of strings.
AEM-5118	Asset root paths are incorrect.	Asset root paths must be a list of strings.

Error code	Error message	Suggested resolution
AEM-5119	Page path inclusion or exclusion patterns are incorrect.	Page name inclusion patterns/ Exclusion must be a list of strings.
AEM-5120	Asset path inclusion or exclusion patterns are incorrect.	Asset name inclusion patterns/ Exclusion must be a list of strings.
AEM-5121	Provided deploymentype is incorrect.	Deployment type should be either CLOUD or ON_PREMISE.
AEM-5122	Provided orgId is incorrect.	OrgId should not be null or empty value.
AEM-5123	Provided technical Account Id is incorrect.	Technical Account Id should not be null or empty value.
AEM-5124	Provided imsHost is incorrect.	IMS Host should not be null or empty value.
AEM-5125	Null/Empty deployment type.	Deployment type should be either CLOUD or ON_PREMISE.
AEM-5126	Invalid Timezone Id.	Provide a valid timezone id.
AEM-5127	Null/empty asset Index field type.	Asset index field should not be null or empty value.
AEM-5128	Null/empty page Index field type.	Page index field should not be null or empty value.
AEM-5129	DataSourceFieldNam e doesn't match with IndexFieldType.	Provide a valid asset indexFieldType for the provided asset dataSourc eFieldName. Or, provide a valid page indexFieldType for the provided page dataSourceFieldName.

Error code	Error message	Suggested resolution
AEM-5130	Protocol used by provided AEM URL is not supported by AEM connector.	Only https protocol is supported by AEM connector. Provide an AEM URL based on https protocol.
AEM-5131	AEM password is too large.	Password should not be greater than 40 characters.
AEM-5132	AEM client ID is too large.	Client ID should not be greater than 40 characters.
AEM-5133	AEM client secret is too large.	Client secret should not be greater than 40 characters.
AEM-5134	AEM private key is too large.	Private key should not be greater than 2048 characters.
AEM-5135	AEM client ID contains invalid characters.	Client ID should not contain unprintable characters.
AEM-5136	AEM client secret contains invalid characters.	Client secret should not contain unprintable characters.
AEM-5137	AEM private key contains invalid characters.	Private key should not contain unprintable characters.
AEM-5138	AEM IMS host is too large.	IMS host should not be greater than 100 characters.
AEM-5139	AEM technical account ID is too large.	Technical account id should not be greater than 100 characters.
AEM-5140	AEM org ID is too large.	Org id should not be greater than 100 characters.

Error code	Error message	Suggested resolution
AEM-5141	Page name inclusion or exclusion patterns are incorrect.	Page name inclusion patterns/ Exclusion must be a list of strings.
AEM-5142	Asset name inclusion or exclusion patterns are incorrect.	Asset name inclusion patterns/ Exclusion must be a list of strings.
AEM-5143	Asset type inclusion or exclusion patterns are incorrect.	Asset type inclusion patterns/Exclusion must be a list of strings.
AEM-5144	Invalid page root path. Please provide valid page root path.	Page path should start with /content.
AEM-5145	Invalid asset root path. Please provide valid asset root path.	Asset path should start with /content/ dam.
AEM-5146	AEM page root paths list size is too large.	Page root paths list size should not be greater than 1000.
AEM-5147	AEM asset root paths list size is too large.	Asset root paths list size should not be greater than 1000.
AEM-5148	Asset root paths list size should not be greater than 1000.	Asset path exclusion patterns list size should not be greater than 1000.
AEM-5149	AEM asset path inclusion pattern list size is too large.	Asset path inclusion patterns list size should not be greater than 1000.
AEM-5150	AEM asset name inclusion pattern list size is too large.	Asset name inclusion patterns list size should not be greater than 1000.

Error code	Error message	Suggested resolution
AEM-5151	AEM asset name exclusion pattern list size is too large.	Asset name exclusion patterns list size should not be greater than 1000.
AEM-5152	AEM asset type exclusion pattern list size is too large.	Asset type exclusion patterns list size should not be greater than 1000.
AEM-5153	AEM asset type inclusion pattern list size is too large.	Asset type inclusion patterns list size should not be greater than 1000.
AEM-5154	AEM page name inclusion pattern list size is too large.	Page name inclusion patterns list size should not be greater than 1000.
AEM-5155	AEM page name Exclusion pattern list size is too large.	Page name exclusion patterns list size should not be greater than 1000.
AEM-5156	AEM page path Exclusion pattern list size is too large.	Page path exclusion patterns list size should not be greater than 1000.
AEM-5157	AEM page path inclusion pattern list size is too large.	Page path inclusion patterns list size should not be greater than 1000.
AEM-5158	AEM page components list size is too large.	Page components list size should not be greater than 1000.
AEM-5159	AEM content fragment variations list size is too large.	Content fragment variations list size should not be greater than 1000.
AEM-5160	AEM host URL characters length is too large.	AEM host URL characters length should not be greater than 2048 characters.

Error code	Error message	Suggested resolution
AEM-5161	Some of the page root paths exceed the character limit.	Page root path characters length should not be greater than 1000.
AEM-5162	Some of the asset root paths exceed the character limit.	Asset root Path characters length should not be greater than 1000 .
AEM-5163	Some of the asset path exclusion objects exceed the character limit.	Asset path exclusion characters length should not be greater than 1000.
AEM-5164	Some of the asset path inclusion objects exceed the character limit.	Asset path inclusion characters length should not be greater than 1000.
AEM-5165	Some of the asset name inclusion objects exceed the character limit.	Asset name inclusion characters length should not be greater than 1000.
AEM-5166	Some of the asset name exclusion objects exceed the character limit.	Asset name exclusion characters length should not be greater than 1000.
AEM-5167	Some of the asset type exclusion objects exceed the character limit.	Asset type exclusion characters length should not be greater than 1000.
AEM-5168	Some of the asset type inclusion objects exceed the character limit.	Asset type inclusion characters length should not be greater than 1000.
AEM-5169	Some of the page name inclusion objects exceed the character limit.	Page name inclusion characters length should not be greater than 1000.

Error code	Error message	Suggested resolution
AEM-5170	Some of the page name exclusion objects exceed the character limit.	Page name exclusion characters length should not be greater than 1000.
AEM-5171	Some of the page path exclusion objects exceed the character limit.	Page path exclusion characters length should not be greater than 1000.
AEM-5172	Some of the page path inclusion objects exceed the character limit.	Page path inclusion characters length should not be greater than 1000.
AEM-5300	Error in serializing change log token.	Retry sync.
AEM-5301	Error in de-serializing change log token.	Retry sync.
AEM-5401	Error occurred while getting AEM groups.	Retry sync.
AEM-5501	Could not connect to host.	
AEM-5502	AEM URL SSRF check failed.	Make sure AEM host URL is not a multicast/local/link-local/loopback address.
AEM-5503	AEM host not found.	Check whether AEM host is up and reachable.
AEM-5504	Error occurred while executing HTTP request against given AEM URL.	Check whether AEM host is up and reachable.
AEM-5505	AEM malformed URL error.	Provide valid AEM url.

Error code	Error message	Suggested resolution
AEM-5506	AEM VPC Configuration check failed.	Site local address is restricted.
AEM-5507	Error in creating document attribute.	Only String, String List, Date and Long formats are supported for field mappings.
AEM-5200	Error occurred while getting pages from AEM for Full Crawl.	Check whether AEM server is up and responding to API requests.
AEM-5506	AEM VPC Configuration check failed.	Site local address is restricted.
AEM-5201	Error occurred while getting assets from AEM for Full Crawl.	Check whether AEM server is up and responding to API requests.
AEM-5303	Error occurred while getting pages from AEM for Change Log.	Check whether AEM server is up and responding to API requests.
AEM-5304	Error occurred while getting assets from AEM for Change Log.	Check whether AEM server is up and responding to API requests.

Connecting Alfresco (Cloud) to Amazon Q Business

Note

Alfresco (Cloud) connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend

exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Alfresco is a content management service (CMS) that helps customers store and manage their content. You can connect Alfresco (Cloud) instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Alfresco (Cloud) connector overview
- Prerequisites for connecting Amazon Q Business to Alfresco (Cloud)
- Connecting Amazon Q Business to Alfresco (Cloud) using the console
- Connecting Amazon Q Business to Alfresco (Cloud) using APIs
- How Amazon Q Business connector crawls Alfresco (Cloud) ACLs
- Alfresco (Cloud) data source connector field mappings
- IAM role for Alfresco (Cloud) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Alfresco (Cloud) connector overview

The following table gives an overview of the Amazon Q Business Alfresco (Cloud) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic, OAuth 2.0 with Client Credentials Flow

Category	Feature	Support
	Authentication credentials	**Basic** • Alfresco username • Alfresco password **OAuth 2.0, with Client Credentials Flow** • Client ID • Client secret • Token URL **Important** Admin privileges required
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Document • Comments See What is a document? for more details on what each connector crawls as a document.

Category	Feature	Support
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include Aspects • Crawl specific Alfresco site • Include/exclude by file path • Include/exclude by file name • Include/exclude by file type
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Alfresco (Cloud)

Before you begin, make sure that you have completed the following prerequisites.

Troubleshooting prerequisites

- /group-members Endpoint Issues: If you experience problems with the /group-members API, upgrade to Alfresco version 7.0 or higher.
- Solr-Related Errors (On-Premises Only): Ensure Solr is properly configured and running. Misconfiguration may result in HTTP 500 errors or failed synchronizations.

In Alfresco, make sure you have:

- Copied your Alfresco repository URL and web application URL. If you only want to index a specific Alfresco site, then also copy the site ID.
- Noted your Alfresco authentication credentials, which include a username and password with at least read permissions. If you want to use OAuth 2.0 authentication, you should add the user to the Alfresco administrators group.

- **Optional**: Generated OAuth 2.0 credentials in Alfresco. The credentials include client ID, client secret, and token URL. For more information about how to configure clients for Alfresco On-Premises, see Alfresco documentation. If you use Alfresco Cloud (PaaS), you must contact Hyland support for Alfresco OAuth 2.0 authentication.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Alfresco (Cloud) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console. Only Alfresco version 7.0 or higher is supported.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Alfresco (Cloud) using the console

The following procedure outlines how to connect Amazon Q Business to Alfresco (Cloud) using the AWS Management Console.

Connecting Amazon Q to Alfresco (Cloud)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Alfresco** data source to your Amazon Q application.
5. Then, on the **Alfresco (Cloud)** data source page, enter the following information:

6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. **Source** – Choose **Alfresco Cloud**.

   a. **Alfresco repository URL** – Enter your Alfresco repository URL. For example, if you use Alfresco Cloud (PaaS), the repository URL could be *https://company.alfrescocloud.com*.

   b. **Alfresco user application URL** – Enter your Alfresco user interface URL. You can get the repository URL from your Alfresco administrator. For example, the user interface URL could be *https://example.com*.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. **Authentication** – Choose **Basic authentication** or **OAuth 2.0 authentication**. Then choose an existing Secrets Manager secret or create a new secret to store your Alfresco credentials. If you choose to create a new secret, an AWS Secrets Manager secret window opens.

   If you chose **Basic authentication**, enter a name for the secret, the Alfresco username, and password.

   If you chose **OAuth 2.0 authentication**, enter a name for the secret, client ID, client secret, and token URL.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

For more information, see VPC.

11. **Identity crawler** – Amazon Q crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.
12. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

13. In **Sync scope**, enter the following information:

a. **Content** – Choose whether to crawl content marked with 'Aspects' in Alfresco, content within a specific Alfresco site, or content across all your Alfresco sites.

b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

c. **Additional configuration – *optional*** – Set the following settings:

- **Include comments** – Choose to include comments in Alfresco Document library and Blog.
- **Regex patterns** – Regular expression patterns to include or exclude certain files.

d. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

15. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.

16. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.

17. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

    For more information, see Field mappings.

18. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Alfresco (Cloud) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Alfresco JSON schema

The following is the Alfresco JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "siteId": {
              "type": "string"
            },
            "repoUrl": {
```

```
            "type": "string"
          },
          "webAppUrl": {
            "type": "string"
          },
          "repositoryAdditionalProperties": {
            "type": "object",
            "properties": {
              "authType": {
                "type": "string",
                "enum": [
                  "OAuth2",
                  "Basic"
                ]
              },
              "type": {
                "type": "string",
                "enum": [
                  "PAAS",
                  "ON_PREM"
                ]
              },
              "crawlType": {
                "type": "string",
                "enum": [
                  "ASPECT",
                  "SITE_ID",
                  "ALL_SITES"
                ]
              }
            }
          }
        }
      }
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "document": {
        "type": "object",
```

```
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": {
                "anyOf": [
                  {
                    "type": "object",
                    "properties": {
                      "indexFieldName": {
                        "type": "string"
                      },
                      "indexFieldType": {
                        "type": "string",
                        "enum": [
                          "STRING",
                          "DATE",
                          "STRING_LIST",
                          "LONG"
                        ]
                      },
                      "dataSourceFieldName": {
                        "type": "string"
                      },
                      "dateFieldFormat": {
                        "type": "string",
                        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                      }
                    },
                    "required": [
                      "indexFieldName",
                      "indexFieldType",
                      "dataSourceFieldName"
                    ]
                  }
                ]
              }
            }
          },
          "required": [
            "fieldMappings"
          ]
        },
        "comment": {
          "type": "object",
```

```
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": {
                "anyOf": [
                  {
                    "type": "object",
                    "properties": {
                      "indexFieldName": {
                        "type": "string"
                      },
                      "indexFieldType": {
                        "type": "string",
                        "enum": [
                          "STRING",
                          "DATE",
                          "STRING_LIST",
                          "LONG"
                        ]
                      },
                      "dataSourceFieldName": {
                        "type": "string"
                      },
                      "dateFieldFormat": {
                        "type": "string",
                        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                      }
                    },
                    "required": [
                      "indexFieldName",
                      "indexFieldType",
                      "dataSourceFieldName"
                    ]
                  }
                ]
              }
            }
          },
          "required": [
            "fieldMappings"
          ]
        }
      }
    },
```

```
    "additionalProperties": {
      "type": "object",
      "properties": {
        "isCrawlAcl": {
          "type": "boolean"
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        },
        "fieldForUserId": {
          "type": "string"
        },
        "aspectName": {
          "type": "string"
        },
        "aspectProperties": {
          "type": "array"
        },
        "enableFineGrainedControl": {
          "type": "boolean"
        },
        "isCrawlComment": {
          "type": "boolean"
        },
        "inclusionFileNamePatterns": {
          "type": "array"
        },
        "exclusionFileNamePatterns": {
          "type": "array"
        },
        "inclusionFileTypePatterns": {
          "type": "array"
        },
        "exclusionFileTypePatterns": {
          "type": "array"
        },
        "inclusionFilePathPatterns": {
          "type": "array"
        },
        "exclusionFilePathPatterns": {
          "type": "array"
        }
      }
    },
```

```
    "type": {
      "type": "string",
      "pattern": "ALFRESCO"
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL"
      ]
    },
    "enableIdentityCrawler": {
      "type": "boolean"
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties",
    "type",
    "secretArn"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the endpoint for the data source.
`repositoryEndpointMetadata`	The endpoint information for the data source.
`siteId`	The identifier of the Alfresco site.
`repoUrl`	The URL of your Alfresco repository. You can get the repository URL from your Alfresco administrator. For example, if you use Alfresco Cloud (PaaS), the repository URL could be *https://company.alfrescocloud.com*. Or, if you use Alfresco On-Premises, the repository URL could be *https://company-alfresco-instance.company-domain.suffix:port*.
`webAppUrl`	The URL of your Alfresco user interface. You can get the Alfresco user interface URL from your Alfresco administrator. For example, the user interface URL could be *https://example.com*.
`repositoryAdditionalProperties`	Additional properties for content in your data source.
`isCrawlAcl`	Specify `true` to crawl access control information from documents. **Note** Amazon Q Business crawls ACL information to ensure responses are generated only from documents your end users have access to by default. See Authorization for more details.

Configuration	Description
fieldForUserId	Specify field to use for UserId for ACL crawling.
authType	The type of authentication that you use, whether OAuth2 or Basic.
type (deployment)	The type of Alfresco that you use, whether PAAS or ON-PREM.
crawlType	The type of content that you want to crawl, whether ASPECT (content marked with 'Aspects' in Alfresco), SITE_ID (content within a specific Alfresco site), or ALL_SITES (content across all your Alfresco sites).
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.
• document • comment	A list of objects that map the attributes or field names of your Alfresco documents and comments to Amazon Q index field names.
additionalProperties	Additional configuration options for your content in your data source.
maxFileSizeInMegaBytes	Specify the Maximum file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
aspectProperties	A list of specific 'Aspects' content that you want to index.
enableFineGrainedControl	true to crawl 'Aspects'.

Configuration	Description
`isCrawlComment`	`true` to index comments.
• `inclusionFileNamePatterns` • `inclusionFileTypePatterns` • `inclusionFilePathPatterns`	A list of regular expression patterns to include certain files in your Alfresco data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.
• `exclusionFileNamePatterns` • `exclusionFileTypePatterns` • `exclusionFilePathPatterns`	A list of regular expression patterns to exclude certain files in your Alfresco data source. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.
`type`	The type of data source. Specify `ALFRESCO` as your data source type.

Configuration	Description

secretArn	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs that are required to connect to your Alfresco. The secret must contain a JSON structure with the following keys:
	
	If using basic authentication:
	
	`{ "username": " username", "password": " password" }`
	
	If using OAuth 2.0 authentication:
	
	`{ "clientId": " client ID", "clientSecret": " client secret", "tokenUrl": " token URL" }`

syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index.

Configuration	Description
`enableIdentityCrawler`	`true` to use the Amazon Q identity crawler to sync identity/principal information on users and groups with access to certain documents. **Note** Amazon Q Business crawls identity information from your data source to ensure responses are generated only from documents end users have access to by default. For more information, see Identity crawler.
`version`	The version of this template that's currently supported.

How Amazon Q Business connector crawls Alfresco (Cloud) ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an Alfresco (Cloud) data source to Amazon Q Business, Amazon Q crawls ACL information attached to a document (user and group information) from your Alfresco (Cloud) instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

The group and user IDs are mapped as follows:

- `_group_ids` – Group IDs exist in Alfresco on files where there are set access permissions. They're mapped from the system names of the groups (not display names) in Alfresco.
- `_user_id` – User IDs exist in Alfresco on files where there are set access permissions. They're mapped from the user emails as the IDs in Alfresco.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Alfresco (Cloud) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application environment and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Alfresco connector supports the following entities and the associated reserved and custom attributes.

Important

If you map any Alfresco (Cloud) field to Amazon Q document title and document body fields, Amazon Q will generate responses from data in the document title and body.

Supported entities and field mappings

- Documents
- Comments

Documents

Alfresco field name	Index field name	Description	Data type
creationTime	_created_at	Default	Date
lastModified	_last_updated_at	Default	Date
author	_authors	Default	String list
sourceUri	_source_uri	Default	String
category	_category	Default	String
fileType	_file_type	Default	String
version	_version	Default	String
siteName	al_site_name	Custom	String
size	al_document_size	Custom	Long (numeric)
versionType	al_version_type	Custom	String
title	al_document_title	Custom	String
repositoryId	al_repository_id	Custom	String

Comments

Alfresco field name	Index field name	Description	Data type
creationTime	_created_at	Default	Date
lastModified	_last_updated_at	Default	Date
author	_authors	Default	String list
sourceUri	_source_uri	Default	String
version	_version	Default	String
category	_category	Default	String
fileType	_file_type	Default	String
siteName	al_site_name	Custom	String
size	al_document_size	Custom	Long (numeric)
versionType	_al_version_type	Custom	String
title	al_document_title	Custom	String
repositoryId	al_repository_id	Custom	String

IAM role for Alfresco (Cloud) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
```

```
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
```

```
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Alfresco (Server) to Amazon Q Business

> **Note**
>
> Alfresco (Server) connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Alfresco is a content management service (CMS) that helps customers store and manage their content. You can connect Alfresco (Server) instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Alfresco (Server) connector overview
- Prerequisites for connecting Amazon Q Business to Alfresco (Server)
- Connecting Amazon Q Business to Alfresco (Server) using the console
- Connecting Amazon Q Business to Alfresco (Server) using APIs
- How Amazon Q Business connector crawls Alfresco (Server) ACLs
- Amazon Q Business Alfresco (Server) data source connector field mappings
- IAM role for Amazon Q Business Alfresco (Server) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.

- For information about connector configuration best practices, see Connector configuration best practices.

Alfresco (Server) connector overview

The following table gives an overview of the Amazon Q Business Alfresco (Server) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic
	Authentication credentials	**Basic** • Alfresco username • Alfresco password
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Document • Comments See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported:

Category	Feature	Support
		• Include Aspects • Crawl specific Alfresco site • Include/exclude by file path • Include/exclude by file name • Include/exclude by file type
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Alfresco (Server)

Before you begin, make sure that you have completed the following prerequisites.

In Alfresco, make sure you have:

- Copied your Alfresco repository URL and web application URL. If you only want to index a specific Alfresco site, then also copy the site ID.
- Noted your Alfresco authentication credentials, which include a username and password with at least read permissions. If you want to use OAuth 2.0 authentication, you should add the user to the Alfresco administrators group.
- **Optional**: Generated OAuth 2.0 credentials in Alfresco. The credentials include client ID, client secret, and token URL. For more information about how to configure clients for Alfresco On-Premises, see Alfresco documentation. If you use Alfresco Cloud (PaaS), you must contact Hyland support for Alfresco OAuth 2.0 authentication.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Alfresco (Server) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Alfresco (Server) using the console

The following procedure outlines how to connect Amazon Q Business to Alfresco (Server) using the AWS Management Console.

Connecting Amazon Q to Alfresco (Server)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Alfresco** data source to your Amazon Q application.
5. Then, on the **Alfresco (Server)** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. **Source** – Choose **Alfresco server**.

   a. **Alfresco repository URL** – Enter your Alfresco repository URL. For example, if you use Alfresco Cloud (PaaS), the repository URL could be *https://company.alfrescocloud.com*.

b. **Alfresco user application URL** – Enter your Alfresco user interface URL. You can get the repository URL from your Alfresco administrator. For example, the user interface URL could be *https://example.com*.

c. **SSL certificate location** – Enter the path to an SSL certificate file stored in an Amazon S3 bucket.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. **Authentication** – Choose **Basic authentication** or **OAuth 2.0 authentication**. Then choose an existing Secrets Manager secret or create a new secret to store your Alfresco credentials. If you choose to create a new secret, an AWS Secrets Manager secret window opens.

   If you chose **Basic authentication**, enter a name for the secret, the Alfresco username, and password.

   If you chose **OAuth 2.0 authentication**, enter a name for the secret, client ID, client secret, and token URL.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **Identity crawler** – Amazon Q crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.

12. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

13. In **Sync scope**, enter the following information:

    a. **Content** – Choose whether to crawl content marked with 'Aspects' in Alfresco, content within a specific Alfresco site, or content across all your Alfresco sites.

    b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

    c. **Additional configuration – *optional*** – Set the following settings:

    - **Include comments** – Choose to include comments in Alfresco Document library and Blog.
    - **Regex patterns** – Regular expression patterns to include or exclude certain files.

    d. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

15. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.

16. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
17. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

18. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Alfresco (Server) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Alfresco JSON schema

The following is the Alfresco JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "siteId": {
              "type": "string"
            },
            "repoUrl": {
              "type": "string"
            },
            "webAppUrl": {
              "type": "string"
            },
            "repositoryAdditionalProperties": {
              "type": "object",
              "properties": {
                "authType": {
                  "type": "string",
                  "enum": [
                    "OAuth2",
                    "Basic"
                  ]
                },
```

```
              "type": {
                "type": "string",
                "enum": [
                  "PAAS",
                  "ON_PREM"
                ]
              },
              "crawlType": {
                "type": "string",
                "enum": [
                  "ASPECT",
                  "SITE_ID",
                  "ALL_SITES"
                ]
              }
            }
          }
        }
      }
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "document": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": {
              "anyOf": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": [
                        "STRING",
```

```
                    "DATE",
                    "STRING_LIST",
                    "LONG"
                  ]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      }
    },
    "required": [
      "fieldMappings"
    ]
  },
  "comment": {
    "type": "object",
    "properties": {
      "fieldMappings": {
        "type": "array",
        "items": {
          "anyOf": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": [
                    "STRING",
```

```
                    "DATE",
                    "STRING_LIST",
                    "LONG"
                  ]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": [
        "fieldMappings"
      ]
    }
  }
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "isCrawlAcl": {
      "type": "boolean"
    },
    "maxFileSizeInMegaBytes": {
      "type": "string"
    },
    "fieldForUserId": {
      "type": "string"
    },
    "aspectName": {
      "type": "string"
    },
```

```
        "aspectProperties": {
          "type": "array"
        },
        "enableFineGrainedControl": {
          "type": "boolean"
        },
        "isCrawlComment": {
          "type": "boolean"
        },
        "inclusionFileNamePatterns": {
          "type": "array"
        },
        "exclusionFileNamePatterns": {
          "type": "array"
        },
        "inclusionFileTypePatterns": {
          "type": "array"
        },
        "exclusionFileTypePatterns": {
          "type": "array"
        },
        "inclusionFilePathPatterns": {
          "type": "array"
        },
        "exclusionFilePathPatterns": {
          "type": "array"
        }
      }
    },
    "type": {
      "type": "string",
      "pattern": "ALFRESCO"
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL"
      ]
```

```
    },
    "enableIdentityCrawler": {
      "type": "boolean"
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties",
    "type",
    "secretArn"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the endpoint for the data source.
`repositoryEndpointMetadata`	The endpoint information for the data source.
`siteId`	The identifier of the Alfresco site.
`repoUrl`	The URL of your Alfresco repository. You can get the repository URL from your Alfresco administrator. For example, if you use Alfresco Cloud (PaaS), the repository URL could be *https://company.alfrescocloud.com*. Or, if you use Alfresco On-Premises, the repository URL could be *https://company-alfresco-instance.company-domain.suffix:port*.

Configuration	Description
webAppUrl	The URL of your Alfresco user interface. You can get the Alfresco user interface URL from your Alfresco administrator. For example, the user interface URL could be *https://example.com*.
repositoryAdditionalProperties	Additional properties for content in your data source.
maxFileSizeInMegaBytes	Specify the Maximum file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
isCrawlAcl	Specify `true` to crawl access control information from documents. **Note** Amazon Q Business crawls ACL information to ensure responses are generated only from documents your end users have access to by default. See Authorization for more details.
fieldForUserId	Specify field to use for `UserId` for ACL crawling.
authType	The type of authentication that you use, whether `OAuth2` or `Basic`.
type (deployment)	The type of Alfresco that you use, whether `PAAS` or `ON-PREM`.

Configuration	Description
`crawlType`	The type of content that you want to crawl, whether `ASPECT` (content marked with 'Aspects' in Alfresco), `SITE_ID` (content within a specific Alfresco site), or `ALL_SITES` (content across all your Alfresco sites).
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.
• `document` • `comment`	A list of objects that map the attributes or field names of your Alfresco documents and comments to Amazon Q index field names.
`additionalProperties`	Additional configuration options for your content in your data source.
`aspectProperties`	A list of specific 'Aspects' content that you want to index.
`enableFineGrainedControl`	`true` to crawl 'Aspects'.
`isCrawlComment`	`true` to index comments.
• `inclusionFileNamePatterns` • `inclusionFileTypePatterns` • `inclusionFilePathPatterns`	A list of regular expression patterns to include certain files in your Alfresco data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.

Configuration	Description
• exclusionFileNamePatterns • exclusionFileTypePatterns • exclusionFilePathPatterns	A list of regular expression patterns to exclude certain files in your Alfresco data source. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.
type	The type of data source. Specify ALFRESCO as your data source type.

secretArn	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs that are required to connect to your Alfresco. The secret must contain a JSON structure with the following keys:
	
	If using basic authentication:
	
	{
	"username": " *username*",
	"password": " *password*"
	}
	
	If using OAuth 2.0 authentication:
	
	{
	"clientId": " *client ID*",
	"clientSecret": " *client secret*",
	"tokenUrl": " *token URL*"
	}

Configuration	Description
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index.
`enableIdentityCrawler`	`true` to use the Amazon Q identity crawler to sync identity/principal information on users and groups with access to certain documents. **Note** Amazon Q Business crawls identity information from your data source to ensure responses are generated only from documents end users have access to by default. For more information, see Identity crawler.
`version`	The version of this template that's currently supported.

How Amazon Q Business connector crawls Alfresco (Server) ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an Alfresco (Server) data source to Amazon Q Business, Amazon Q crawls ACL information attached to a document (user and group information) from your Alfresco (Server) instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

The group and user IDs are mapped as follows:

- `_group_ids` – Group IDs exist in Alfresco on files where there are set access permissions. They're mapped from the system names of the groups (not display names) in Alfresco.
- `_user_id` – User IDs exist in Alfresco on files where there are set access permissions. They're mapped from the user emails as the IDs in Alfresco.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Amazon Q Business Alfresco (Server) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source

attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application environment and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Alfresco connector supports the following entities and the associated reserved and custom attributes.

> **Important**
>
> If you map any Alfresco (Server) field to Amazon Q document title and document body fields, Amazon Q will generate responses from data in the document title and body.

Supported entities and field mappings

- Documents
- Comments

Documents

Alfresco field name	Index field name	Description	Data type
creationTime	_created_at	Default	Date
lastModified	_last_updated_at	Default	Date
author	_authors	Default	String list
sourceUri	_source_uri	Default	String
category	_category	Default	String
fileType	_file_type	Default	String

Alfresco field name	Index field name	Description	Data type
version	_version	Default	String
siteName	al_site_name	Custom	String
size	al_document_size	Custom	Long (numeric)
versionType	al_version_type	Custom	String
title	al_document_title	Custom	String
repositoryId	al_repository_id	Custom	String

Comments

Alfresco field name	Index field name	Description	Data type
creationTime	_created_at	Default	Date
lastModified	_last_updated_at	Default	Date
author	_authors	Default	String list
sourceUri	_source_uri	Default	String
version	_version	Default	String
category	_category	Default	String
fileType	_file_type	Default	String
siteName	al_site_name	Custom	String
size	al_document_size	Custom	Long (numeric)
versionType	_al_version_type	Custom	String
title	al_document_title	Custom	String

Alfresco field name	Index field name	Description	Data type
repositoryId	al_repository_id	Custom	String

IAM role for Amazon Q Business Alfresco (Server) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
```

```
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
```

```
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
```

```
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
"qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
"qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
```

```
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Aurora (MySQL) to Amazon Q Business

> **Note**
>
> Aurora (MySQL) connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Aurora (MySQL) is a relational database management system (RDBMS) built for the cloud. You can connect your Aurora (MySQL) instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

The Amazon Q Aurora (MySQL) data source connector supports Aurora MySQL 3 and Aurora Serverless MySQL 8.0.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials. Also, avoid adding tables with sensitive data or personal identifiable information (PII).

Topics

- Known limitations for the Aurora (MySQL) connector
- Aurora (MySQL) connector overview
- Prerequisites for connecting Amazon Q Business to Aurora (MySQL)
- Connecting Amazon Q Business to Aurora (MySQL) using the console
- Connecting Amazon Q Business to Aurora (MySQL) using APIs
- How Amazon Q Business connector crawls Aurora (MySQL) ACLs
- Aurora (MySQL) data source connector field mappings
- IAM role for Aurora (MySQL) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Aurora (MySQL) connector

The Aurora (MySQL) connector has the following known limitations:

- Deleted database rows will not be tracked in when Amazon Q checks for updated content.
- The size of field names and values in a row of your database can't exceed 400KB.
- Column names should only contain alphanumeric characters and not spaces.
- If you have a large amount of data in your database data source, and do not want Amazon Q to index all your database content after the first sync, you can choose to sync only new, modified, or deleted documents.

Aurora (MySQL) connector overview

The following table gives an overview of the Amazon Q Business Aurora (MySQL) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic
	Authentication credentials	• Username of database user • Password of database user
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Driver version	MySQL – 8.0.2.7
	Data source version	Aurora MySQL 3, Aurora Serverless MySQL 8.0

Category	Feature	Support
	Identity crawling	No
	VPC	Yes
Crawl features	Custom metadata	Yes
	Entities	Yes. The following entities are supported: • Document **Note** Each database row is considered an individual searchable Amazon Q document. See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Aurora (MySQL)

Before you begin, make sure that you have completed the following prerequisites.

In Aurora (MySQL), make sure you have:

- Noted your database username and password.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials.

- Copied your database host URL, port, and instance. You can find this information on the Amazon RDS console.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Aurora (MySQL) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Aurora (MySQL) using the console

The following procedure outlines how to connect Amazon Q Business to Aurora (MySQL) using the AWS Management Console.

Connecting Amazon Q to Aurora (MySQL)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Aurora (MySQL)** data source to your Amazon Q application.

5. Then, on the **Aurora (MySQL)** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. In **Source**, enter the following information:

   a. **Host** – Enter the database host URL, for example: `http://instance URL.region.rds.amazonaws.com`.

   b. **Port** – Enter the database port, for example, `5432`.

   c. **Instance** – Enter the database instance, for example `postgres`.

   d. **SSL certificate location** – Choose to enter the Amazon S3 path to your SSL certificate file.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
9. In **Authentication**, enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. For **Database username**, and **Password** – Enter the authentication credential values you copied from your database.

   c. Choose **Save**.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

12. In **Sync scope**, enter the following information:

- **SQL query** – Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
- **Primary key column** – Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
- **Title column** – Provide the column in your database table that contains the document titles.
- **Body column** – Provide the column in your database table that contains the document body text.

  Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

> **Important**
>
> Place the entire SQL statement on a single line. For example:
>
> ```
> SELECT column1, column2, column3 FROM table_name WHERE condition;
> ```
>
> Queries with line breaks will cause errors.

13. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Additional configuration – *optional*** – Configure the following settings:

    - **Change-detecting columns** – Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns.
    - **Users' IDs column** – Enter the name of the column which contains User IDs to be allowed access to content.
    - **Groups column** – Enter the name of the column that contains groups to be allowed access to content.
    - **Source URLs column** – Enter the name of the column which contains Source URLs to be indexed.
    - **Time stamps column** – Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
    - **Time zones column** – Enter the name of the column which contains time zones for the content to be crawled.
    - **Time stamps format** – Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.

15. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New or modified content sync** – Sync only new and modified documents.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

    For more details, see Sync mode.

16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
18. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages,

including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Aurora (MySQL) using APIs

You use the `CreateDataSource` action to connect a data source to your Amazon Q application.

Then, you use the `configuration` parameter to provide a JSON schema with all other configuration information specific to your data source connector.

Aurora (MySQL) JSON schema

The following is the Aurora (MySQL) JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            },
            "dbInstance": {
```

```
            "type": "string"
          }
        },
        "required": [
          "dbType",
          "dbHost",
          "dbPort",
          "dbInstance"
        ]
      }
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "document": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string"
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
```

```
            }
          },
          "required": [
            "fieldMappings"
          ]
        }
      },
      "required": [
      ]
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "primaryKey": {
          "type": "string"
        },
        "titleColumn": {
          "type": "string"
        },
        "bodyColumn": {
          "type": "string"
        },
        "sqlQuery": {
          "type": "string",
          "not": {
            "pattern": ";+"
          }
        },
        "timestampColumn": {
          "type": "string"
        },
        "timestampFormat": {
          "type": "string"
        },
        "timezone": {
          "type": "string"
        },
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
```

```
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "serverlessAurora": {
          "type": "string",
          "enum": ["true", "false"]
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
```

```
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
connectionConfiguration	Configuration information for the endpoint for the data source.
repositoryEndpointMetadata	Required configuration information for connecting your data source. • dbType—The type of Java database you are using, whether `mysql`, db2, `postgresql` , `oracle`, or `sqlserver` . • dbHost—The database host name. • dbPort—The database port. • dbInstance—The database instance.
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings. Specify the type of data source and the secret ARN.
document	A list of objects that map the attributes or field names of your database content to Amazon Q index field names. For more information, see Fiel.
additionalProperties	Additional configuration options for your content in your data source. Use to include or

Configuration	Description
	exclude specific content in your database data source.
primaryKey	Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
titleColumn	Provide the name of the column in your database table that you want to designate as the column with document titles.
bodyColumn	Provide the name of the column in your database table that you want to designate as the column with document body text. Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.
sqlQuery	Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
timestampColumn	Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
timestampFormat	Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.

Configuration	Description
timezone	Enter the name of the column which contains time zones for the content to be crawled.
changeDetectingColumns	Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns
allowedUsersColumns	Enter the name of the column which contains User IDs to be allowed access to content.
allowedGroupsColumn	Enter the name of the column which contains User IDs to be allowed access to content.
sourceURIColumn	Enter the name of the column which contains Source URLs to be indexed.
isSslEnabled	`true` to add a path to an SSL certificate file stored in an Amazon S3 bucket.
type	The type of data source. Specify `JDBC` as your data source type.

Configuration	Description
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose • `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.
secretArn	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains username and password required to connect to your database. The secret must contain a JSON structure with the following keys: `{ "username": " database username", "password": " password" }`
version	The version of the template that is currently supported.

How Amazon Q Business connector crawls Aurora (MySQL) ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect a database data source to Amazon Q, Amazon Q crawls user and group information from a column in the source table. You specify this column in the console or using the `configuration` parameter as part of the `CreateDataSource` operation.

If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

A database data source has the following limitations:

- You can only specify an allow list for a database data source. You can't specify a deny list.
- You can only specify groups. You can't specify individual users for the allow list.
- The database column should be a string containing a semicolon delimited list of groups.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Aurora (MySQL) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional

document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q PostgreSQL connector supports the following field mappings:

Supported field mappings

- Document

Document

JDBC field name	Index field name	Description	Data type
jd_document_id	jd_document_id	Custom	String
jd_document_title	jd_document_title	Custom	String
jd_source_uri	_source_uri	Default	String

IAM role for Aurora (MySQL) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
```

```
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Aurora (PostgreSQL) to Amazon Q Business

> **Note**
>
> Aurora (PostgreSQL) connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Aurora (PostgreSQL) is a relational database management system (RDBMS) built for the cloud. You can connect your Aurora (PostgreSQL) instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

The Amazon Q Aurora (PostgreSQL) data source connector supports Aurora PostgreSQL 1.

Important

As a best practice, provide Amazon Q with read-only database credentials. Also, avoid adding tables with sensitive data or personal identifiable information (PII).

Topics

- Known limitations for the Aurora (PostgreSQL) connector
- Aurora (PostgreSQL) connector overview
- Prerequisites for connecting Amazon Q Business to Aurora (PostgreSQL)
- Connecting Amazon Q Business to Aurora (PostgreSQL) using the console
- Connecting Amazon Q Business to Aurora (PostgreSQL) using APIs
- How Amazon Q Business connector crawls Aurora (PostgreSQL) ACLs
- Aurora (PostgreSQL) data source connector field mappings
- IAM role for Aurora (PostgreSQL) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Aurora (PostgreSQL) connector

The Aurora (PostgreSQL) connector has the following known limitations:

- Deleted database rows will not be tracked in when Amazon Q checks for updated content.
- The size of field names and values in a row of your database can't exceed 400KB.
- Column names should only contain alphanumeric characters and not spaces.

- If you have a large amount of data in your database data source, and do not want Amazon Q to index all your database content after the first sync, you can choose to sync only new, modified, or deleted documents.

Aurora (PostgreSQL) connector overview

The following table gives an overview of the Amazon Q Business Aurora (PostgreSQL) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic
	Authentication credentials	• Username of database user • Password of database user
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Driver version	Aurora (PostgreSQL) – 42.3.2
	Data source version	Aurora PostgreSQL 1
	Identity crawling	No
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Document **Note** Each database row is considered an individual searchable Amazon Q document.

Category	Feature	Support
		See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Aurora (PostgreSQL)

Before you begin, make sure that you have completed the following prerequisites.

In Aurora (PostgreSQL), make sure you have:

- Noted your database username and password.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials.

- Copied your database host URL, port, and instance. You can find this information on the Amazon RDS console.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Aurora (PostgreSQL) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Aurora (PostgreSQL) using the console

The following procedure outlines how to connect Amazon Q Business to Aurora (PostgreSQL) using the AWS Management Console.

Connecting Amazon Q to Aurora (PostgreSQL)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Aurora (PostgreSQL)** data source to your Amazon Q application.
5. Then, on the **Aurora (PostgreSQL)** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, enter the following information:

   a. **Host** – Enter the database host URL, for example: `http://instance URL.region.rds.amazonaws.com`.

b. **Port** – Enter the database port, for example, 5432.

c. **Instance** – Enter the database instance

d. **Enable SSL certificate location** – Choose to enter the Amazon S3 path to your SSL certificate file.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. In **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

a. **Secret name** – A name for your secret.

b. For **Database username**, and **Password** – Enter the authentication credential values you copied from your database.

c. Choose **Save**.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

12. In **Sync scope**, enter the following information:

- **SQL query** – Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
- **Primary key column** – Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
- **Title column** – Provide the name of the column in your database table that you want to designate as the column with document titles.
- **Body column** – Provide the name of the column in your database table that you want to designate as the column with document body text.

  Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

13. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Additional configuration – *optional*** – Configure the following settings:

    - **Change-detecting columns** – Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns.
    - **Users' IDs column** – Enter the name of the column which contains User IDs to be allowed access to content.
    - **Groups column** – Enter the name of the column that contains groups to be allowed access to content.
    - **Source URLs column** – Enter the name of the column which contains Source URLs to be indexed.
    - **Time stamps column** – Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.

- **Time zones column** – Enter the name of the column which contains time zones for the content to be crawled.
- **Time stamps format** – Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.

15. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New or modified content sync** – Sync only new and modified documents.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

    For more details, see Sync mode.

16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
18. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Aurora (PostgreSQL) using APIs

You use the `CreateDataSource` action to connect a data source to your Amazon Q application.

Then, you use the `configuration` parameter to provide a JSON schema with all other configuration information specific to your data source connector.

Aurora (PostgreSQL) JSON schema

The following is the Aurora (PostgreSQL) JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
```

```
            "type": "string",
            "enum": [
              "mysql",
              "db2",
              "postgresql",
              "oracle",
              "sqlserver"
            ]
          },
          "dbHost": {
            "type": "string"
          },
          "dbPort": {
            "type": "string"
          },
          "dbInstance": {
            "type": "string"
          }
        },
        "required": [
          "dbType",
          "dbHost",
          "dbPort",
          "dbInstance"
        ]
      }
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "document": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string"
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
```

```
        "timestampColumn": {
          "type": "string"
        },
        "timestampFormat": {
          "type": "string"
        },
        "timezone": {
          "type": "string"
        },
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "serverlessAurora": {
          "type": "string",
          "enum": ["true", "false"]
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
```

```
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
connectionConfiguration	Configuration information for the endpoint for the data source.
repositoryEndpointMetadata	Required configuration information for connecting your data source. • dbType—The type of Java database you are using, whether `mysql`, db2, `postgresql` , `oracle`, or `sqlserver` . • dbHost—The database host name. • dbPort—The database port. • dbInstance—The database instance.

Configuration	Description
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings. Specify the type of data source and the secret ARN.
document	A list of objects that map the attributes or field names of your database content to Amazon Q index field names. For more information, see Fiel.
additionalProperties	Additional configuration options for your content in your data source. Use to include or exclude specific content in your database data source.
primaryKey	Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
titleColumn	Provide the name of the column in your database table that you want to designate as the column with document titles.
bodyColumn	Provide the name of the column in your database table that you want to designate as the column with document body text. Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

Configuration	Description
sqlQuery	Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
timestampColumn	Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
timestampFormat	Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.
timezone	Enter the name of the column which contains time zones for the content to be crawled.
changeDetectingColumns	Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns
allowedUsersColumns	Enter the name of the column which contains User IDs to be allowed access to content.
allowedGroupsColumn	Enter the name of the column which contains User IDs to be allowed access to content.
sourceURIColumn	Enter the name of the column which contains Source URLs to be indexed.
isSslEnabled	`true` to add a path to an SSL certificate file stored in an Amazon S3 bucket.
type	The type of data source. Specify `JDBC` as your data source type.

Configuration	Description
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose • `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.
secretArn	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains username and password required to connect to your database. The secret must contain a JSON structure with the following keys: `{ "username": " database username", "password": " password" }`
version	The version of the template that is currently supported.

How Amazon Q Business connector crawls Aurora (PostgreSQL) ACLs

When you connect a database data source to Amazon Q Business, Amazon Q Business crawls user and group information from a column in the source table. You specify this column in the console or using the `configuration` parameter as part of the `CreateDataSource` operation.

Activating ACL crawling allows the system to filter chat responses based on your end users' document access levels.

Prerequisites:

- The group ACL column in the database should be a string containing a semicolon delimited list of groups.
- The user ACL column in the database should be a string containing a semicolon delimited list of users.

A database data source has the following limitation:

- You can only specify an allow list for a database data source. You can't specify a deny list.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Aurora (PostgreSQL) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source

attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q PostgreSQL connector supports the following field mappings:

Supported field mappings

- Document

Document

JDBC field name	Index field name	Description	Data type
jd_document_id	jd_document_id	Custom	String
jd_document_title	jd_document_title	Custom	String
jd_source_uri	_source_uri	Default	String

IAM role for Aurora (PostgreSQL) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
```

```
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Drupal to Amazon Q Business

> **Note**
>
> Drupal connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Drupal is an open-source content management system (CMS) that you can use to create websites and web applications. You can connect Drupal instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Drupal connector overview
- Prerequisites for connecting Amazon Q Business to Drupal
- Connecting Amazon Q Business to Drupal using the console
- Connecting Amazon Q Business to Drupal using APIs
- How Amazon Q Business connector crawls Drupal ACLs
- Drupal data source connector field mappings
- IAM role for Drupal connector
- Known limitations for the Drupal connector
- Understand error codes in the Drupal connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Drupal connector overview

The following table gives an overview of the Amazon Q Business Drupal connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic, OAuth 2.0 with Client Credentials Flow
	Authentication credentials	**Basic** • Username • Password • Client email

Category	Feature	Support
		• Private key **OAuth 2.0 with Client Credentials Flow** • Username • Password • Client ID • Client Secret
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Contents • Comments • Attachments See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports default and custom field mappings. For more information, see Field mappings.

Category	Feature	Support
	Filters	Yes. The following filters are supported: • Include/ exclude articles, article comments, and article attachments • Include/exclude basic pages, basic page comments, and basic page attachments • Include/exclude basic blocks, basic block comments, and basic block attachments • Include custom content types • Include custom blocks • Include/exclude content by article title, basic page title, basic block title, custom content title, custom block title, and file name
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Drupal

Before you begin, make sure that you have completed the following prerequisites.

In Drupal, make sure you have:

- Created a Drupal (Standard) Suite account and a user with an administrator role.
- Install the *Web Services* modules from Drupal's core modules. These include the *HTTP Basic Authentication module*, the *JSON:API* module, the *RESTful Web Services* module, and the *Serialization* module.
- Configure the *JSON:API* module to accept the JSON:API *create*, *read*, *update*, and *delete* operations.
- Copied your Drupal site name and configured a host URL. For example, *https://<hostname>/<drupalsitename>*.

- Configured basic authentication credentials containing a username (Drupal website login username) and password (Drupal website password).
- **Recommended:** Configured an OAuth 2.0 credential token. Use this token along with your Drupal password grant, client id, client secret, username (Drupal website login username) and password (Drupal website password) to connect to Amazon Q.
- Added the following permissions in your Drupal account using an administrator role:
  - administer blocks
  - administer block_content display
  - administer block_content fields
  - administer block_content form display
  - administer views
  - view user email addresses
  - view own unpublished content
  - view page revisions
  - view article revisions
  - view all revisions
  - view the administration theme
  - access content
  - access content overview
  - access comments
  - search content
  - access files overview
  - access contextual links

> **Note**
>
> If there are user defined content types or user defined block types, or any views and blocks are added to the Drupal website, they must be provided with administrator access.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.

- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Drupal authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Drupal using the console

The following procedure outlines how to connect Amazon Q Business to Drupal using the AWS Management Console.

Connecting Amazon Q to Drupal

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Drupal** data source to your Amazon Q application.
5. Then, on the **Drupal** data source page, enter the following information:
6. **Name and description**, do the following:

    - For **Data source name** – Name your data source for easy tracking.

    > **Note**
    >
    > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. In **Source**, for **Host URL** – Enter the host URL of your Drupal site. For example, *https://<hostname>/<drupalsitename>*.
8. **SSL certificate location** – Enter the path to the SSL certificate stored in an Amazon S3 bucket. You use this to connect to Drupal with a secure SSL connection.
9. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
10. **Authentication** – Choose between **Basic authentication** and **OAuth 2.0 authentication** and then enter the following information for your **AWS Secrets Manager secret**.

    a. **Basic authentication** – Enter the **User name**, (Drupal site username), and **Password** (Drupal site password).

    b. **OAuth 2.0 authentication** – Enter the **User name**, (Drupal site username), and **Password** (Drupal site password).

11. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

12. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

13. In **Sync scope**, enter the following information:

    a. For **Select entities**:

    - **Articles**—Choose whether to crawl **Articles**, their comments **Comments**, and their **Attachments**.
    - **Basic pages**—Choose whether to crawl **Basic pages**, their **Comments**, and their **Attachments**.
    - **Basic blocks**—Choose whether to crawl **Basic blocks**, their **Comments**, and their **Attachments**.
    - You can also choose to add and crawl **Custom content types** and **Custom Blocks**.

    b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

    c. (Optional) **Additional configuration** – Configure the following settings:

    - **Regex pattern**—Add regular expression patterns to include or exclude specific entity titles and file names. You can add up to 100 patterns.

    d. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. For **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync**—Sync all content regardless of the previous sync status.
    - **New, modified, or deleted content sync**—Sync only new, modified, and deleted documents.

15. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.

16. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
17. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

18. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Drupal using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Drupal JSON schema

The following is the Drupal JSON schema:

```
{
 "$schema": "http://json-schema.org/draft-04/schema#",
 "type": "object",
 "properties": {
  "connectionConfiguration": {
   "type": "object",
   "properties": {
    "repositoryEndpointMetadata": {
     "type": "object",
     "properties": {
      "hostUrl": {
       "type": "string",
       "pattern": "https:.*"
      }
     },
     "required": [
      "hostUrl"
     ]
    }
   },
   "required": [
    "repositoryEndpointMetadata"
   ]
  },
  "repositoryConfigurations": {
   "type": "object",
   "properties": {
    "content": {
     "type": "object",
```

```
      "properties": {
       "fieldMappings": {
        "type": "array",
        "items": [
         {
          "type": "object",
          "properties": {
           "indexFieldName": {
            "type": "string"
           },
           "indexFieldType": {
            "type": "string",
            "enum": [
             "STRING",
             "DATE"
            ]
           },
           "dataSourceFieldName": {
            "type": "string"
           },
           "dateFieldFormat": {
            "type": "string",
            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
           }
          },
          "required": [
           "indexFieldName",
           "indexFieldType",
           "dataSourceFieldName"
          ]
         }
        ]
       }
      },
      "required": [
       "fieldMappings"
      ]
     },
     "comment": {
      "type": "object",
      "properties": {
       "fieldMappings": {
        "type": "array",
        "items": [
```

```
        {
         "type": "object",
         "properties": {
          "indexFieldName": {
           "type": "string"
          },
          "indexFieldType": {
           "type": "string",
           "enum": [
            "STRING",
            "DATE"
           ]
          },
          "dataSourceFieldName": {
           "type": "string"
          },
          "dateFieldFormat": {
           "type": "string",
           "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
         },
         "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
         ]
        }
       ]
      }
     },
     "required": [
      "fieldMappings"
     ]
    },
    "attachment": {
     "type": "object",
     "properties": {
      "fieldMappings": {
       "type": "array",
       "items": [
        {
         "type": "object",
         "properties": {
          "indexFieldName": {
```

```
          "type": "string"
         },
         "indexFieldType": {
          "type": "string",
          "enum": [
           "STRING",
           "DATE"
          ]
         },
         "dataSourceFieldName": {
          "type": "string"
         },
         "dateFieldFormat": {
          "type": "string",
          "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
         }
        },
        "required": [
         "indexFieldName",
         "indexFieldType",
         "dataSourceFieldName"
        ]
       }
      ]
     }
    },
    "required": [
     "fieldMappings"
    ]
   }
  }
 },
 "additionalProperties": {
  "type": "object",
  "properties": {
   "isCrawlAcl": {
    "type": "boolean"
   },
   "maxFileSizeInMegaBytes": {
    "type": "string"
   },
   "fieldForUserId": {
    "type": "string"
   },
```

```
    "isCrawlArticle": {
     "type": "boolean"
    },
    "isCrawlBasicPage": {
     "type": "boolean"
    },
    "isCrawlBasicBlock": {
     "type": "boolean"
    },
    "crawlCustomContentTypesList": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "crawlCustomBlockTypesList": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "filePath": {
     "anyOf": [
      {
       "type": "string",
       "pattern": "s3:.*"
      },
      {
       "type": "string",
       "pattern": ""
      }
     ]
    },
    "inclusionFileNamePatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "exclusionFileNamePatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
```

```
    },
    "articleTitleInclusionPatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "articleTitleExclusionPatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "pageTitleInclusionPatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "pageTitleExclusionPatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "customContentTitleInclusionPatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "customContentTitleExclusionPatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "basicBlockTitleInclusionPatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "basicBlockTitleExclusionPatterns": {
```

```
      "type": "array",
      "items": {
       "type": "string"
      }
     },
     "customBlockTitleInclusionPatterns": {
      "type": "array",
      "items": {
       "type": "string"
      }
     },
     "customBlockTitleExclusionPatterns": {
      "type": "array",
      "items": {
       "type": "string"
      }
     },
     "contentDefinitions": {
      "type": "array",
      "items": {
       "properties": {
        "contentType": {
         "type": "string"
        },
        "fieldDefinition": {
         "type": "array",
         "items": [
          {
           "type": "object",
           "properties": {
            "machineName": {
             "type": "string"
            },
            "type": {
             "type": "string"
            }
           },
           "required": [
            "machineName",
            "type"
           ]
          }
         ]
        },
```

```
        "isCrawlComments": {
         "type": "boolean"
        },
        "isCrawlFiles": {
         "type": "boolean"
        }
       }
      },
      "required": [
       "contentType",
       "fieldDefinition",
       "isCrawlComments",
       "isCrawlFiles"
      ]
     }
    },
    "required": []
   },
   "type": {
    "type": "string",
    "pattern": "DRUPAL"
   },
   "authType": {
    "type": "string",
    "enum": [
     "BASIC-AUTH",
     "OAUTH2"
    ]
   },
   "syncMode": {
    "type": "string",
    "enum": [
     "FORCED_FULL_CRAWL",
     "FULL_CRAWL",
     "CHANGE_LOG"
    ]
   },
   "enableIdentityCrawler": {
    "type": "boolean"
   },
   "secretArn": {
    "type": "string",
    "minLength": 20,
    "maxLength": 2048
```

```
  }
 },
 "version": {
  "type": "string",
  "anyOf": [
   {
    "pattern": "1.0.0"
   }
  ]
 },
 "required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
  "additionalProperties",
  "secretArn",
  "type"
 ]
}
```

The following provides information on important JSON keys to configure.

Configuration	Description
connectionConfiguration	Configuration information for the endpoint for the data source.
repositoryEndpointMetadata	The endpoint information for the data source.
hostUrl	The host URL of your Drupal website. For example, *https://<hostname>/<drupalsitename>* .
repositoryConfigurations	Configuration information for the content of the data source.
• content • comment •	A list of objects that map the attributes or field names of your Drupal files. The Drupal data source field names must exist in your Drupal custom metadata.

Configuration	Description
attachment	
additionalProperties	Additional configuration options for your content in your data source.
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
`isCrawlAcl`	Specify `true` to crawl access control informati on from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.

Configuration	Description
• inclusionFileNamePatterns • articleTitleInclusionPatterns • pageTitleInclusionPatterns • customContentTitleInclusionPatterns • basicBlockTitleInclusionPatterns • customBlockTitleInclusionPatterns	A list of regular expression patterns to *include* certain files in your Drupal data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.
• exclusionFileNamePatterns • articleTitleExclusionPatterns • pageTitleExclusionPatterns • customContentTitleExclusionPatterns • basicBlockTitleExclusionPatterns • customBlockTitleExclusionPatterns	A list of regular expression patterns to *exclude* certain files in your Drupal data source. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an exclusion and inclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.

Configuration	Description
contentDefinitions • contentType • fieldDefinition • isCrawlComments • isCrawlFiles • isCrawlArticle • isCrawlBasicPage • isCrawlBasicBlock • isCrawlCustomContentTypesList	Specify the content types to crawl and whether to crawl comments and attachments for your selected content types.
type	The type of data source. Specify `DRUPAL` as your data source type.
authType	The type of authentication you are using, whether `BASIC-AUTH` or `OAUTH2`.

Configuration	Description
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose • `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to certain documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.

Configuration	Description

secretARN	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains the key-value pairs required to connect to your Drupal. The secret must contain a JSON structure with the following keys:
	
	If using basic authentication:
	
	`{ "user name": "user name", "passwords": "password" }`
	
	If using OAuth 2.0 authentication:
	
	`{ "Client ID": "client_id" , "Client secret": "client_secret" , "user name": "user name", "password": "password" }`

version	The version of this template that is currently supported.

How Amazon Q Business connector crawls Drupal ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an Drupal data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your Drupal instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

Amazon Q gets the user and group information from the Drupal instance.The group and user IDs are mapped as follows:

- `_group_ids` – Group IDs exist in Drupal on files where there are set access permissions. They are mapped from the names of the groups in Drupal.
- `_user_id` – User IDs exist in Drupal on files where there are set access permissions. They are mapped from the user emails as the IDs in Drupal.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Drupal data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

Important

Filtering using document attributes in chat is only supported through the API.

The Amazon Q Drupal connector supports the following entities and the associated reserved and custom attributes.

Supported entities and field mappings

- Contents
- Comments
- Attachments

Contents

Drupal field name	Index field name	Entity	Category	Field type
title	dpl_title	All Entities	Default	String
sourceUrl	dpl_source_url	All Entities	Default	String
createdAt	dpl_created_date	All Entities	Default	Date
updatedAt	dpl_updated_date	All Entities	Default	Date
published	dpl_published	All Entities	Default	String
tag	dpl_tag	All Entities	Default	String
author	dpl_author	All Entities	Default	String
category	dpl_category	All Entities	Default	String
visibility	dpl_visibility	All Entities	Default	String
viewId	dpl_view_id	All Entities	Default	String

Comments

Drupal field name	Index field name	Entity	Category	Field type
title	dpl_comment_title	All Entities	Default	String
sourceUrl	dpl_source_url	All Entities	Default	String
createdAt	dpl_created_date	All Entities	Default	Date
updatedAt	dpl_updated_date	All Entities	Default	Date
approvedStatus	dpl_status	All Entities	Default	String
author	dpl_author	All Entities	Default	String
category	dpl_category	All Entities	Default	String
parentEntityId	dpl_parent_entity_id	All Entities	Default	String
visibility	dpl_visibility	All Entities	Default	String
viewId	dpl_view_id	All Entities	Default	String

Attachments

Drupal field name	Index field name	Entity	Category	Field type
fileName	dpl_file_name	All Entities	Default	String
sourceUrl	dpl_source_url	All Entities	Default	String

Drupal field name	Index field name	Entity	Category	Field type
createdAt	dpl_created_date	All Entities	Default	Date
updatedAt	dpl_updated_date	All Entities	Default	Date
status	dpl_status	All Entities	Default	String
fileType	dpl_file_type	All Entities	Default	String
fileSize	dpl_file_size	All Entities	Default	String
fileUploadedBy	dpl_file_uploaded_by	All Entities	Default	String
category	dpl_category	All Entities	Default	String
parentEntityId	dpl_parent_entity_id	All Entities	Default	String
visibility	dpl_visibility	All Entities	Default	String
viewId	dpl_view_id	All Entities	Default	String

IAM role for Drupal connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
```

```
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Known limitations for the Drupal connector

Amazon Q Business Drupal connector has the following known limitations:

- Drupal APIs have no official throttling limits.
- Java SDKs are not available for Drupal.
- Drupal data can be fetched only using native JSON API's.
- Content types not associated with any Drupal **View** cannot be crawled.
- You need administrator access to crawl data from Drupal **Blocks**.
- There is no JSON API available to create the user defined content type using HTTP verbs.
- The document body and comments for **Articles**, **Basic pages**, **Basic blocks**, user defined content type, and user defined block type, are displayed in HTML format. If the HTML content is not well-formed, then the HTML related tags will appear in the document body and comments and will be visible in Amazon Kendra search results.

- Content types and **Block** types without description or body will not be ingested into Amazon Q. Only **Comments** and **Attachments** of such **Content** or **Block** types will be ingested into your Amazon Q index.

Understand error codes in the Drupal connector

The following table provides information about error codes you may see for the Drupal connector and suggested resolutions.

Error code	Error message	Suggested resolution
DPL-5001	Invalid userName or password while validating credentials.	Provide valid values for the userName and password.
DPL-5002	Invalid userName or password while validating OAuth credentials.	Provide valid userName and password.
DPL-5003	Invalid clientId or clientSecret while validating OAuth credentials.	Provide valid clientId and clientSecret.
DPL-5100	Empty/null host URL	The hostUrl should not be null or empty.
DPL-5101	Null/empty username.	Provide a valid userName.
DPL-5102	Null/empty password.	Provide a valid password.
DPL-5103	Null/empty ClientId.	Provide a valid clientId.
DPL-5104	Null/empty Client Secret.	Provide a valid clientSecret.
DPL-5105	Incorrect auth type in the repositoryAdditionalProperties.	The authType should be basicAuth or OAuth2.

Error code	Error message	Suggested resolution
DPL-5106	Null/empty auth type in the repositoryAdditionalProperties.	The authType should not be null or empty.
DPL-5107	Null/empty Repository Configurations.	The repositoryConfigurations should not be null or empty.
DPL-5108	Only String, String List, Date and Long formats are supported for the indexFieldType in all the field mappings.	Provide the supported format only for the indexFieldType in all the fieldMappings.
DPL-5109	Not able to read the file from the S3 bucket location.	Check if valid JSON file is provided in the repositoryAdditionalProperties.
DPL-5110	Invalid Profile Name provided.	Provide a valid s3ProfileName in the repositoryAdditionalProperties. For example, default
DPL-5111	Null/empty Profile Name.	The s3ProfileName should not be null/empty in the repositoryAdditionalProperties.
DPL-5112	Invalid URI found during address validation.	Provide a valid hostUrl.
DPL-5131	Null/empty ContentTypes/BlockTypes in contentDefinitions.	Provide value for the contentType or blockType in contentDefinitions.
DPL-5132	Null/empty/unknown field definitions in the contentDefinitions.	The fieldDefinition should be an empty array only.

Error code	Error message	Suggested resolution
DPL-5133	Invalid field definitions in the contentDefinitions.	In the contentDefinitions, the fieldDefinition should be a json array only having machineName and type fields.
DPL-5134	Null/empty value found for the machineName in the fieldDefinition.	Provide value for the machineName in the fieldDefinition.
DPL-5135	Null/empty value found for the type in the fieldDefinition.	Provide value for the type in the fieldDefinition.
DPL-5136	Invalid isCrawlComments value.	isCrawlComments should be a boolean value true or false.
DPL-5137	Invalid isCrawlFiles value.	isCrawlFiles should be a boolean value true or false.
DPL-5138	The machineName is not found in the fieldDefinition.	Define the machineName as key in the fieldDefinition.
DPL-5139	The type is not found in the fieldDefinition.	Define the type as key in the fieldDefinition.
DPL-5151	Invalid inclusion file name patterns	Provide valid regex pattern in the inclusionFileNamePatterns.
DPL-5152	Invalid exclusion file name patterns.	Provide valid regex pattern in the exclusionFileNamePatterns.
DPL-5153	Invalid Article title inclusion patterns.	Provide valid regex pattern in the articleTitleInclusionPatterns.
DPL-5154	Invalid Article title exclusion patterns.	Please provide valid regex pattern in the articleTitleExclusionPatterns.

Error code	Error message	Suggested resolution
DPL-5155	Invalid Page title inclusion filter patterns.	Provide valid regex pattern in the pageTitleInclusionPatterns.
DPL-5156	Invalid Page title exclusion filter patterns.	Provide valid regex pattern in the pageTitleExclusionPatterns.
DPL-5157	Invalid Custom Content title inclusion filter patterns.	Provide valid regex pattern in the customContentTitleInclusionPatterns.
DPL-5158	Invalid Custom Content title exclusion filter patterns.	Provide valid regex pattern in the customContentTitleExclusionPatterns.
DPL-5159	Invalid Basic Block title inclusion filter patterns.	Provide valid regex pattern in the basicBlockTitleInclusionPatterns.
DPL-5160	Invalid Basic Block title exclusion filter patterns.	Provide valid regex pattern in the basicBlockTitleExclusionPatterns.
DPL-5161	Invalid Custom Block title inclusion filter patterns.	Provide valid regex pattern in the customBlockTitleInclusionPatterns.
DPL-5162	Invalid Custom Block title exclusion filter patterns.	Provide valid regex pattern in the customBlockTitleExclusionPatterns.
DPL-5200	IO Exception occurred while reading contents from Drupal.	Refer to the log for more details.
DPL-5201	Please try again later. Unknown exception occurred.	Unknown exception occurred. Refer to the log for more details.

Error code	Error message	Suggested resolution
DPL-5202	Issue occurred while initializing Views with acl info in the cache for content entity:	Issue with Views. Refer to the log for more details.
DPL-5203	Drupal Configuration found null during change access token of OAuth authentication.	Issue with OAuth Authentication. Refer to the log for more details.
DPL-5204	The generated access token is empty or null. Issue occurred while generating access token.	Access token should not be null/empty. Provide valid access token and try. If still issue exists, refer to the log for more details.
DPL-5205	User info with the given userName do not exist.	Verify the provided userName and correct it.
DPL-5206	The api response has empty data element.	Check the logs for details about empty response body.
DPL-5207	Either no records found or some issue with View filter criteria for content entity:	Refer to the log for more details.
DPL-5500	Drupal connection successful.	Drupal connection successful.

Connecting IBM DB2 to Amazon Q Business

Note

IBM DB2 connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more

scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

IBM DB2 is a relational database management system developed by IBM. If you are a AWS user, you can use Amazon Q Business to index your IBM DB2 data source.

You can connect your IBM DB2 instance to Amazon Q—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

The Amazon Q IBM DB2 data source connector supports DB2 11.5.7.

Important

As a best practice, provide Amazon Q with read-only database credentials. Also, avoid adding tables with sensitive data or personal identifiable information (PII).

Topics

- Known limitations for the IBM DB2 connector
- IBM DB2 connector overview
- Prerequisites for connecting Amazon Q Business to IBM DB2
- Connecting Amazon Q Business to IBM DB2 using the console
- Connecting Amazon Q Business to IBM DB2 using APIs
- How Amazon Q Business connector crawls IBM DB2 ACLs
- IBM DB2 data source connector field mappings
- IAM role for IBM DB2 connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.

- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the IBM DB2 connector

The IBM DB2 connector has the following known limitations:

- Deleted database rows will not be tracked in when Amazon Q checks for updated content.
- The size of field names and values in a row of your database can't exceed 400KB.
- Column names should only contain alphanumeric characters and not spaces.
- If you have a large amount of data in your database data source, and do not want Amazon Q to index all your database content after the first sync, you can choose to sync only new, modified, or deleted documents.

IBM DB2 connector overview

The following table gives an overview of the IBM DB2 connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic
	Authentication credentials	• Username of database user • Password of database user
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Driver version	DB2 – 11.5.7.0
	Data source version	11.5.7
	Identity crawling	No
	VPC	Yes
Crawl features	**Custom metadata**	Yes

Category	Feature	Support
	Entities	Yes. The following entities are supported: • Document **Note** Each database row is considered an individual searchable Amazon Q document. See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to IBM DB2

Before you begin, make sure that you have completed the following prerequisites.

In IBM DB2, make sure you have:

- Noted your database username and password.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials.

- Copied your database host URL, port, and instance.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your IBM DB2 authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to IBM DB2 using the console

The following procedure outlines how to connect Amazon Q Business to IBM DB2 using the AWS Management Console.

Connecting Amazon Q to IBM DB2

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **IBM DB2** data source to your Amazon Q application.
5. Then, on the **IBM DB2** data source page, enter the following information:
6. **Name and description**, do the following:

    - For **Data source name** – Name your data source for easy tracking.

    > **Note**
    >
    > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. In **Source**, enter the following information:

   a. **Host** – Enter the database host name.

   b. **Port** – Enter the database port.

   c. **Instance** – Enter the database instance.

   d. **Enable SSL certificate location** – Choose to enter the Amazon S3 path to your SSL certificate file.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. In **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. For **Database username**, and **Password** – Enter the authentication credential values you copied from your database.

   c. Choose **Save**.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

12. In **Sync scope**, enter the following information:

    - **SQL query** – Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
    - **Primary key column** – Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
    - **Title column** – Provide the name of the column in your database table that you want to designate as the column with document titles.
    - **Body column** – Provide the name of the column in your database table that you want to designate as the column with document body text.

      Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

13. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Additional configuration – *optional*** – Configure the following settings:

    - **Change-detecting columns** – Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns.
    - **Users' IDs column** – Enter the name of the column which contains User IDs to be allowed access to content.

- **Groups column** – Enter the name of the column that contains groups to be allowed access to content.
- **Source URLs column** – Enter the name of the column which contains Source URLs to be indexed.
- **Time stamps column** – Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
- **Time zones column** – Enter the name of the column which contains time zones for the content to be crawled.
- **Time stamps format** – Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.

15. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New or modified content sync** – Sync only new and modified documents.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

    For more details, see Sync mode.
16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
18. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to IBM DB2 using APIs

You use the `CreateDataSource` action to connect a data source to your Amazon Q application.

Then, you use the `configuration` parameter to provide a JSON schema with all other configuration information specific to your data source connector.

IBM DB2 JSON schema

The following is the IBM DB2 JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
```

```
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            },
            "dbInstance": {
              "type": "string"
            }
          },
          "required": [
            "dbType",
            "dbHost",
            "dbPort",
            "dbInstance"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "document": {
```

```
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string"
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": [
            "fieldMappings"
          ]
        }
      },
      "required": [
      ]
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "primaryKey": {
          "type": "string"
        },
        "titleColumn": {
          "type": "string"
        },
```

```
        "bodyColumn": {
          "type": "string"
        },
        "sqlQuery": {
          "type": "string",
          "not": {
            "pattern": ";+"
          }
        },
        "timestampColumn": {
          "type": "string"
        },
        "timestampFormat": {
          "type": "string"
        },
        "timezone": {
          "type": "string"
        },
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "serverlessAurora": {
          "type": "string",
          "enum": ["true", "false"]
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
```

```
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
connectionConfiguration	Configuration information for the endpoint for the data source.
repositoryEndpointMetadata	Required configuration information for connecting your data source.

Configuration	Description
	• dbType—The type of Java database you are using, whether `mysql`, db2, `postgresql` , `oracle`, or `sqlserver` . • dbHost—The database host name. • dbPort—The database port. • dbInstance—The database instance.
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings. Specify the type of data source and the secret ARN.
document	A list of objects that map the attributes or field names of your database content to Amazon Q index field names. For more information, see Fiel.
additionalProperties	Additional configuration options for your content in your data source. Use to include or exclude specific content in your database data source.
primaryKey	Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
titleColumn	Provide the name of the column in your database table that you want to designate as the column with document titles.

Configuration	Description
bodyColumn	Provide the name of the column in your database table that you want to designate as the column with document body text. Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.
sqlQuery	Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
timestampColumn	Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
timestampFormat	Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.
timezone	Enter the name of the column which contains time zones for the content to be crawled.
changeDetectingColumns	Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns
allowedUsersColumns	Enter the name of the column which contains User IDs to be allowed access to content.
allowedGroupsColumn	Enter the name of the column which contains User IDs to be allowed access to content.

Configuration	Description
sourceURIColumn	Enter the name of the column which contains Source URLs to be indexed.
isSslEnabled	`true` to add a path to an SSL certificate file stored in an Amazon S3 bucket.
type	The type of data source. Specify `JDBC` as your data source type.
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose • `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.
secretArn	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains username and password required to connect to your database. The secret must contain a JSON structure with the following keys: `{ "username": " database username", "password": " password" }`

Configuration	Description
version	The version of the template that is currently supported.

How Amazon Q Business connector crawls IBM DB2 ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect a database data source to Amazon Q, Amazon Q crawls user and group information from a column in the source table. You specify this column in the console or using the `configuration` parameter as part of the `CreateDataSource` operation.

If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

A database data source has the following limitations:

- You can only specify an allow list for a database data source. You can't specify a deny list.
- You can only specify groups. You can't specify individual users for the allow list.
- The database column should be a string containing a semicolon delimited list of groups.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

IBM DB2 data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q PostgreSQL connector supports the following field mappings:

Supported field mappings

- Document

Document

JDBC field name	Index field name	Description	Data type
jd_document_id	jd_document_id	Custom	String
jd_document_title	jd_document_title	Custom	String
jd_source_uri	_source_uri	Default	String

IAM role for IBM DB2 connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
```

```
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
```

```
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
```

```
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
"qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Microsoft SQL Server to Amazon Q Business

> **Note**
>
> Microsoft SQL Server connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we

recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Microsoft SQL Server is an relational database management system (RDBMS) developed by Microsoft. You can connect your Microsoft SQL Server instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

The Amazon Q Microsoft SQL Server data source connector supports MS SQL Server 2019.

Important

As a best practice, provide Amazon Q with read-only database credentials. Also, avoid adding tables with sensitive data or personal identifiable information (PII).

Topics

- Known limitations for the Microsoft SQL Server connector
- Microsoft SQL Server connector overview
- Prerequisites for connecting Amazon Q Business to Microsoft SQL Server
- Connecting to Microsoft SQL Server using the console
- Connecting to Microsoft SQL Server using APIs
- How connector crawls Microsoft SQL Server ACLs
- Microsoft SQL Server data source connector field mappings
- IAM role for Microsoft SQL Server connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.

- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Microsoft SQL Server connector

The Microsoft SQL Server connector has the following known limitations:

- Deleted database rows will not be tracked in when Amazon Q checks for updated content.
- The size of field names and values in a row of your database can't exceed 400KB.
- Column names should only contain alphanumeric characters and not spaces.
- If you have a large amount of data in your database data source, and do not want Amazon Q to index all your database content after the first sync, you can choose to sync only new, modified, or deleted documents.

Microsoft SQL Server connector overview

The following table gives an overview of the Amazon Q Business Microsoft SQL Server connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic
	Authentication credentials	• Username of database user • Password of database user
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Driver version	Microsoft SQL Server – 10.2.0.jre11
	Data source version	SQL Server 2019
	Identity crawling	No
	VPC	Yes
Crawl features	**Custom metadata**	Yes

Category	Feature	Support
	Entities	Yes. The following entities are supported: • Document **Note** Each database row is considered an individual searchable Amazon Q document. See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Microsoft SQL Server

Before you begin, make sure that you have completed the following prerequisites.

In Microsoft SQL Server, make sure you have:

- Noted your database username and password.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials.

- Copied your database host URL, port, and instance.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Microsoft SQL Server authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting to Microsoft SQL Server using the console

The following procedure outlines how to connect Amazon Q Business to Microsoft SQL Server using the AWS Management Console.

Connecting Amazon Q to Microsoft SQL Server

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Microsoft SQL Server** data source to your Amazon Q application.
5. Then, on the **Microsoft SQL Server** data source page, enter the following information:
6. **Name and description**, do the following:

    - For **Data source name** – Name your data source for easy tracking.

    > **Note**
    >
    > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. In **Source**, enter the following information:

   a. **Host** – Enter the database host name.

   b. **Port** – Enter the database port.

   c. **Instance** – Enter the database instance.

   d. **Enable SSL certificate location** – Choose to enter the Amazon S3 path to your SSL certificate file.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. In **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. For **Database username**, and **Password** – Enter the authentication credential values you copied from your database.

   c. Choose **Save**.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

12. In **Sync scope**, enter the following information:

    - **SQL query** – Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
    - **Primary key column** – Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
    - **Title column** – Provide the name of the column in your database table that you want to designate as the column with document titles.
    - **Body column** – Provide the name of the column in your database table that you want to designate as the column with document body text.

      Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

13. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Additional configuration – *optional*** – Configure the following settings:

    - **Change-detecting columns** – Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns.
    - **Users' IDs column** – Enter the name of the column which contains User IDs to be allowed access to content.

- **Groups column** – Enter the name of the column that contains groups to be allowed access to content.
- **Source URLs column** – Enter the name of the column which contains Source URLs to be indexed.
- **Time stamps column** – Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
- **Time zones column** – Enter the name of the column which contains time zones for the content to be crawled.
- **Time stamps format** – Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.

15. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New or modified content sync** – Sync only new and modified documents.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

    For more details, see Sync mode.
16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
18. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting to Microsoft SQL Server using APIs

You use the `CreateDataSource` action to connect a data source to your Amazon Q application.

Then, you use the `configuration` parameter to provide a JSON schema with all other configuration information specific to your data source connector.

Microsoft SQL Server JSON schema

The following is the Microsoft SQL Server JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
```

```
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            },
            "dbInstance": {
              "type": "string"
            }
          },
          "required": [
            "dbType",
            "dbHost",
            "dbPort",
            "dbInstance"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "document": {
```

```
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string"
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": [
            "fieldMappings"
          ]
        }
      },
      "required": [
      ]
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "primaryKey": {
          "type": "string"
        },
        "titleColumn": {
          "type": "string"
        },
```

```
        "bodyColumn": {
          "type": "string"
        },
        "sqlQuery": {
          "type": "string",
          "not": {
            "pattern": ";+"
          }
        },
        "timestampColumn": {
          "type": "string"
        },
        "timestampFormat": {
          "type": "string"
        },
        "timezone": {
          "type": "string"
        },
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "serverlessAurora": {
          "type": "string",
          "enum": ["true", "false"]
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
```

```
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL"
      ]
    },
    "secretArn": {
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
connectionConfiguration	Configuration information for the endpoint for the data source.
repositoryEndpointMetadata	Required configuration information for connecting your data source. • dbType—The type of Java database you are using, whether `mysql`, db2, `postgresql` , `oracle`, or `sqlserver` .

Configuration	Description
	• dbHost—The database host name. • dbPort—The database port. • dbInstance—The database instance.
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings. Specify the type of data source and the secret ARN.
document	A list of objects that map the attributes or field names of your database content to Amazon Q index field names. For more information, see Mapping data source fields.
additionalProperties	Additional configuration options for your content in your data source. Use to include or exclude specific content in your database data source.
primaryKey	Provide the primary key for the database table. This identifies a table within your database.
titleColumn	Provide the name of the document title column within your database table.
bodyColumn	Provide the name of the document title column within your database table.

Configuration	Description
sqlQuery	Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query. If a table name has special characters, put it in square brackets "[ ]" in the SQL query. For example: `select * from [my-database-table]` .
timestampColumn	Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
timestampFormat	Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.
timezone	Enter the name of the column which contains time zones for the content to be crawled.
changeDetectingColumns	Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns
allowedUsersColumns	Enter the name of the column which contains User IDs to be allowed access to content.
allowedGroupsColumn	Enter the name of the column which contains User IDs to be allowed access to content.
sourceURIColumn	Enter the name of the column which contains Source URLs to be indexed.

Configuration	Description
isSslEnabled	`true` to add a path to an SSL certificate file stored in an Amazon S3 bucket.
type	The type of data source. Specify `JDBC` as your data source type.
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose • `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.
secretArn	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains user name and password required to connect to your database. The secret must contain a JSON structure with the following keys: `{ "username": " database username", "password": " password" }`
version	The version of the template that is currently supported.

How connector crawls Microsoft SQL Server ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect a database data source to Amazon Q, Amazon Q crawls user and group information from a column in the source table. You specify this column in the console or using the `configuration` parameter as part of the `CreateDataSource` operation.

If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

A database data source has the following limitations:

- You can only specify an allow list for a database data source. You can't specify a deny list.
- You can only specify groups. You can't specify individual users for the allow list.
- The database column should be a string containing a semicolon delimited list of groups.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Microsoft SQL Server data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q PostgreSQL connector supports the following field mappings:

Supported field mappings

- Document

Document

JDBC field name	Index field name	Description	Data type
jd_document_id	jd_document_id	Custom	String
jd_document_title	jd_document_title	Custom	String
jd_source_uri	_source_uri	Default	String

IAM role for Microsoft SQL Server connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
```

```
            ]
        },
        {
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Microsoft Yammer to Amazon Q Business

> **Note**
>
> Microsoft Yammer connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Microsoft Yammer is an enterprise collaboration tool for messaging, meetings, and file sharing. You can connect Microsoft Yammer instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the Microsoft Yammer connector
- Microsoft Yammer connector overview
- Prerequisites for connecting Amazon Q to Microsoft Yammer
- Connecting Amazon Q Business to Microsoft Yammer using the console
- Connecting Amazon Q Business to Microsoft Yammer using APIs
- How Amazon Q Business connector crawls Microsoft Yammer ACLs
- Microsoft Yammer data source connector field mappings
- IAM role for Microsoft Yammer connector
- Understand error codes in the Microsoft Yammer connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Microsoft Yammer connector

The Microsoft Yammer connector has the following known limitations:

- Due to API limitations, an incremental sync will not update deleted **Messages**, **Attachments**, **Communities** and **Users**. To update deleted entities, you must run a full sync.

Microsoft Yammer connector overview

The following table gives an overview of the Microsoft Yammer connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	OAuth 2.0 with Resource Owner Password Flow
	Authentication credentials	• Microsoft Yammer username • Microsoft Yammer password • Microsoft Yammer Client ID • Microsoft Yammer Client secret
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Message • Attachment • User • Community See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Community names • Public messages

Category	Feature	Support
		• Attachments • Inbox private messages • Crawl content beginning from a date • Including and excluding content by file type
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q to Microsoft Yammer

Before you begin, make sure that you have completed the following prerequisites.

In Microsoft Yammer, make sure you have:

- Created a Microsoft Yammer administrative account with verified admin user permissions.
- Configured an OAuth 2.0 credential token containing a client ID and client secret.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Microsoft Yammer authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Microsoft Yammer using the console

The following procedure outlines how to connect Amazon Q Business to Microsoft Yammer using the AWS Management Console.

Connecting Amazon Q to Microsoft Yammer

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Microsoft Yammer** data source to your Amazon Q application.
5. Then, on the **Microsoft Yammer** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
8. **Authentication** – Choose between **New** and **Existing**.

   - If you choose **Existing**, select an existing secret for **Select secret**.

     If you choose **New**, enter the following information in the **New AWS Secrets Manager secret** section:

     - **Secret name** – A name for your secret.
     - **Username** – The username for your Microsoft Yammer Active Directory account.

- **Password** – The password for your Microsoft Yammer Active Directory account.
- **Client ID** – The OAuth client ID credential values you copied from your Microsoft Yammer account.
- **Client secret** – The client secret from your Microsoft Yammer account.

9. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

   a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

   b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

   For more information, see VPC.

10. **Identity crawler** – Amazon Q crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

   For more information, see IAM role.

12. For **Sync scope**, provide the following information:

- **sinceDate** – Select the date in your data source content from when Amazon Q should begin to crawl your data.
- **Select content to sync** – Choose between **All**, **Public messages**, **Attachments**, and **Inbox private messages**.

13. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

14. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

15. For **Additional configuration – *optional***, provide the following information:

    - **Community names** – Enter the community names you wish to include in your application.
    - **Regex patterns** – Add regular expression patterns to include or exclude certain file types. You can add up to 100 patterns.

16. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New or modified content sync** – Sync only new and modified documents.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

    For more details, see Sync mode.

17. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.

18. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.

19. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

20. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Microsoft Yammer using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Yammer JSON schema

The following is the Yammer JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
          }
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "community": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": {
                "anyOf": [
                  {
                    "type": "object",
                    "properties": {
                      "indexFieldName": {
                        "type": "string"
                      },
                      "indexFieldType": {
                        "type": "string",
                        "enum": [
                          "STRING",
                          "DATE"
                        ]
                      },
```

```
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          }
        },
        "required": [
          "fieldMappings"
        ]
      },
      "user": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": {
              "anyOf": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": [
                        "STRING",
                        "DATE"
                      ]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
```

```
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          }
        },
        "required": [
          "fieldMappings"
        ]
      },
      "message": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": {
              "anyOf": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": [
                        "STRING",
                        "DATE"
                      ]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
```

```
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "attachment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": {
            "anyOf": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "DATE"
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
```

```
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "isCrawlAcl": {
        "type": "boolean"
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "fieldForUserId": {
        "type": "string"
      },
      "inclusionPatterns": {
        "type": "array"
      },
      "exclusionPatterns": {
        "type": "array"
      },
      "sinceDate": {
        "type": "string",
        "pattern": "^(19|2[0-9])[0-9]{2}-(0[1-9]|1[012])-(0[1-9]|[12][0-9]|
3[01])T(0[0-9]|1[0-9]|2[0-3]):([0-5][0-9]):([0-5][0-9])((\\+|-)(0[0-9]|1[0-9]|2[0-3]):
([0-5][0-9]))?$"
      },
      "communityNameFilter": {
        "type": "array",
```

```
          "items": {
            "type": "string"
          }
        },
        "isCrawlMessage": {
          "type": "boolean"
        },
        "isCrawlAttachment": {
          "type": "boolean"
        },
        "isCrawlPrivateMessage": {
          "type": "boolean"
        }
      },
      "required": [
        "sinceDate"
      ]
    },
    "type": {
      "type": "string",
      "pattern": "YAMMER"
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "useChangeLog": {
      "type": "string",
      "enum": [
        "true",
        "false"
      ]
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "enableIdentityCrawler": {
      "type": "boolean"
```

```
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties",
    "type",
    "secretArn",
    "syncMode"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the data source.
`repositoryEndpointMetadata`	The endpoint information for the data source. This data source doesn't specify an endpoint in `repositoryEndpointMetadata` . Rather, the connection information is included in an AWS Secrets Manager secret that you provide the `secretArn` .
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.
• `community` • `user` • `message`	A list of objects that map attributes or field names of Microsoft Yammer objects to Amazon Q index field names.

Configuration	Description
• attachment	
secretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Microsoft Yammer data source. This includes your client ID and client secret.
additionalProperties	Additional configuration options for your content in your data source
isCrawlAcl	Specify true to crawl access control informati on from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.
maxFileSizeInMegaBytes	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
fieldForUserId	Specify field to use for UserId for ACL crawling.
• isCrawlMessage • isCrawlAttachment • isCrawlPrivateMessage	Input TRUE to index

Configuration	Description
• `sinceDate`	Use to specify the time from when Amazon Q should crawl your Microsoft Yammer content
• `communityNameFilter`	Use to specify community names to index.
`inclusionPatterns`	A list of regular expression patterns to *include* specific files in your Yammer data source. Files that match the patterns are included in the index. File that don't match the patterns are excluded from the index. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.
`exclusionPatterns`	A list of regular expression patterns to *exclude* specific files in your Yammer data source. Files that match the patterns are excluded from the files in your data source. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an exclusion and inclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.
`type`	Specify `YAMMER` as your data source type
`useChangeLog`	`true` to use the Yammer change log to determine which documents require adding, updating, or deleting in the index.

Configuration	Description
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to certain documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.

How Amazon Q Business connector crawls Microsoft Yammer ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an Microsoft Yammer data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your Microsoft Yammer instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

The group and user IDs are mapped as follows:

- `_email_id` – Your Microsoft email ID is an identifier that's necessary to configure each connector instance. Your email ID can be found in the properties section of your Microsoft account dashboard.
- `_group_id` – Group IDs exist in Microsoft Yammer Instances where there are set access permissions. They're mapped from the names of the groups in Microsoft Yammer.

- Authorization
- Identity crawler
- Understanding User Store

Microsoft Yammer data source connector field mappings

To help you structure data for retrieval and chat filtering, Amazon Q Business crawls data source document attributes or metadata and maps them to fields in your Amazon Q index.

Amazon Q has reserved fields that it uses when querying your application. When possible, Amazon Q automatically maps these built-in fields to attributes in your data source. If a built-in field doesn't have a default mapping, or if you want to map additional index fields, use the custom field mappings to specify how a data source attribute maps to your Amazon Q application. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

Important

Filtering using document attributes in chat is only supported through the API.

The Amazon Q Yammer connector supports the following entities and the associated reserved and custom attributes.

Note

You can map any Yammer field to the document title or document body Amazon Q reserved/default index fields.

Supported entities and field mappings

- Message
- Attachment
- User
- Community

Message

Amazon Q supports crawling Microsoft Yammer Messages and offers the following message field mappings.

Microsoft Yammer field name	Index field name	Description	Data type
id	ymr_id	Custom	String
message_type	ymr_message_type	Custom	String
api_url	ymr_api_url	Custom	String
group_id	ymr_group_id	Custom	String
group_name	ymr_group_name	Custom	String

Microsoft Yammer field name	Index field name	Description	Data type
in_private_conversation	ymr_in_private_conversation	Custom	String
in_private_group	ymr_in_private_group	Custom	String
sender_email	ymr_sender_email	Custom	String
sender_id	ymr_sender_id	Custom	String
sender_name	ymr_sender_name	Custom	String
created_at	_created_at	Default	Date
web_url	_source_uri	Default	String

Attachment

Microsoft Yammer field name	Index field name	Description	Data type
id	ymr_attachment_id	Custom	String
name	ymr_attachment_name	Custom	String
size	ymr_attachment_size	Custom	String
url	ymr_attachment_url	Custom	String
file_type	ymr_attachment_type	Custom	String
created_at	_created_at	Default	Date

Microsoft Yammer field name	Index field name	Description	Data type
privacy	ymr_attachment_privacy	Custom	String
group_name	ymr_attachment_group_name	Custom	String
sender_email	ymr_attachment_sender_email	Custom	String
web_url	_source_uri	Default	String

User

Microsoft Yammer field name	Index field name	Description	Data type
id	ymr_user_id	Custom	String
user_type	ymr_user_type	Custom	String
state	ymr_user_state	Custom	String
full_name	ymr_user_full_name	Custom	String
activated_at	_created_at	Default	Date
first_name	ymr_user_first_name	Custom	String
last_name	ymr_user_last_name	Custom	String
network_name	ymr_user_network_name	Custom	String
network_domains	ymr_user_network_domains	Custom	String

Microsoft Yammer field name	Index field name	Description	Data type
url	ymr_user_url	Custom	String
name	ymr_user_name	Custom	String
birth_date	ymr_user_birth_date	Custom	Date
admin	ymr_user_admin	Custom	String
verified_admin	ymr_user_verified_admin	Custom	String
contact	ymr_user_contact	Custom	String
email	ymr_user_email	Custom	String
web_url	_source_uri	Default	String

Community

Microsoft Yammer field name	Index field name	Description	Data type
id	ymr_community_id	Custom	String
name	ymr_community_name	Custom	String
email	ymr_community_email	Custom	String
full_name	ymr_community_full_name	Custom	String
description	ymr_community_description	Custom	String

Microsoft Yammer field name	Index field name	Description	Data type
privacy	ymr_community_privacy	Custom	String
url	ymr_community_url	Custom	String
created_at	_created_at	Default	Date
state	ymr_community_state	Custom	String
web_url	_source_uri	Default	String

IAM role for Microsoft Yammer connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
```

```
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
```

```
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the Microsoft Yammer connector

The following table provides information about error codes you may see for the Microsoft Yammer connector and suggested resolutions.

Error code	Error message	Suggested resolution
YMR-5001	Authentication error.	Provide a valid client id, client secret, username, password.

Error code	Error message	Suggested resolution
YMR-5002	Error validating credentials due to invalid username or password.	Provide a valid username and password.
YMR-5003	Error validating credentials due to invalid client id or client secret.	Provide valid client id and client secret.
YMR-5004	Access token is empty or null .	Provide non-empty or non-null access token .
YMR-5100	Null/empty client id.	Provide client id.
YMR-5101	Null/empty client secret.	Provide client secret.
YMR-5102	Null/empty username.	Provide username.
YMR-5103	Null/empty password.	Provide password .
YMR-5104	Null/empty since date.	Provide sinceDate .
YMR-5105	invalid sinceDate format.	since date format should be like YYYY-MM-DDTHH:mm:ss+00:00.
YMR-5106	Empty/null Repository configurations.	Provide Repository configurations.
YMR-5107	Empty/null message entity in repository configuration.	Provide message entity in repository configuration.
YMR-5108	Empty/null Attachment entity in repository configuration.	Provide attachment entity in repository configuration.
YMR-5109	Empty/null message entity field mapping.	Provide message entity field mapping.

Error code	Error message	Suggested resolution
YMR-5110	Empty/null attachment entity field mapping.	Provide attachment entity field mapping.
YMR-5111	Empty/null indexFiel dName, indexFieldType or dataSourceFieldName in message entity.	Provide value for indexFieldName, indexFieldType and dataSourc eFieldName in message entity.
YMR-5112	Empty/null indexFiel dName, indexFieldType or dataSourceFieldName in attachment entity.	Provide value for indexFieldName, indexFieldType and dataSourc eFieldName in message entity.
YMR-5113	Invalid patterns in the regex.	Provide valid regex patterns.
YMR-5114	Since date should be less than current date.	Provide since date less than current date.
YMR-5115	Only String, Date and Long formats are supported for field mappings.	Provide String, Date and Long formats for field mappings.
YMR-5116	Null/empty Network Domain.	Provide Network Domain.
YMR-5117	Got error while building groups.	Refer to logs for more information.
YMR-5118	Configuration found null during change access token.	Please provide valid configurations.
YMR-5119	Unable to connect to Yammer account.	Refer to logs for more details.

Error code	Error message	Suggested resolution
YMR-5120	An error occurred during the test connection.	Refer to logs for more details.
YMR-5500	Bad zip entry.	Provide a valid zip file.
YMR-5501	Invalid URI.	Provide valid URI.
YMR-5502	ContinuableInterna lServerError.	Try again later.

Connecting MySQL to Amazon Q Business

Note

MySQL connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

MySQL is an open source relational database management system. You can connect your MySQL instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

The Amazon Q MySQL data source connector supports MySQL 8.0. 21.

Important

As a best practice, provide Amazon Q with read-only database credentials. Also, avoid adding tables with sensitive data or personal identifiable information (PII).

Topics

- Known limitations for the MySQL connector

- MySQL connector overview
- Prerequisites for connecting Amazon Q Business to MySQL
- Connecting Amazon Q Business to MySQL using the console
- Connecting Amazon Q Business to MySQL using APIs
- How Amazon Q Business connector crawls MySQL ACLs
- MySQL data source connector field mappings
- IAM role for MySQL connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the MySQL connector

- Deleted database rows will not be tracked in when Amazon Q checks for updated content.
- The size of field names and values in a row of your database can't exceed 400KB.
- Column names should only contain alphanumeric characters and not spaces.
- If you have a large amount of data in your database data source, and do not want Amazon Q to index all your database content after the first sync, you can choose to sync only new, modified, or deleted documents.

MySQL connector overview

The following table gives an overview of the Amazon Q Business MySQL connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic
	Authentication credentials	• Username of database user • Password of database user
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Driver version	MySQL – 8.0.27
	Data source version	MySQL 8.0.21
	Identity crawling	No
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Document **Note** Each database row is considered an individual searchable Amazon Q document. See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Sync mode	Supports full and incremental sync.

Category	Feature	Support
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to MySQL

Before you begin, make sure that you have completed the following prerequisites.

In MySQL, make sure you have:

- Noted your database username and password.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials.

- Copied your database host URL, port, and instance.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your MySQL authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to MySQL using the console

The following procedure outlines how to connect Amazon Q Business to MySQL using the AWS Management Console.

Connecting Amazon Q to MySQL

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **MySQL** data source to your Amazon Q application.
5. Then, on the **MySQL** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, enter the following information:

   a. **Host** – Enter the database host name.

   b. **Port** – Enter the database port.

   c. **Instance** – Enter the database instance.

   d. **Enable SSL certificate location** – Choose to enter the Amazon S3 path to your SSL certificate file.
8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
9. In **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

a. **Secret name** – A name for your secret.

b. For **Database username**, and **Password** – Enter the authentication credential values you copied from your database.

c. Choose **Save**.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

    For more information, see IAM role.

12. In **Sync scope**, enter the following information:

- **SQL query** – Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
- **Primary key column** – Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
- **Title column** – Provide the name of the column in your database table that you want to designate as the column with document titles.
- **Body column** – Provide the name of the column in your database table that you want to designate as the column with document body text.

Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

13. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Additional configuration – *optional*** – Configure the following settings:

    - **Change-detecting columns** – Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns.
    - **Users' IDs column** – Enter the name of the column which contains User IDs to be allowed access to content.
    - **Groups column** – Enter the name of the column that contains groups to be allowed access to content.
    - **Source URLs column** – Enter the name of the column which contains Source URLs to be indexed.
    - **Time stamps column** – Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
    - **Time zones column** – Enter the name of the column which contains time zones for the content to be crawled.
    - **Time stamps format** – Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.

15. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New or modified content sync** – Sync only new and modified documents.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

For more details, see Sync mode.

16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
18. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.

You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to MySQL using APIs

You use the `CreateDataSource` action to connect a data source to your Amazon Q application.

Then, you use the `configuration` parameter to provide a JSON schema with all other configuration information specific to your data source connector.

MySQL JSON schema

The following is the MySQL JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
```

```
            },
            "dbInstance": {
              "type": "string"
            }
          },
          "required": [
            "dbType",
            "dbHost",
            "dbPort",
            "dbInstance"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "document": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string"
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
```

```
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
      "timestampColumn": {
        "type": "string"
      },
      "timestampFormat": {
        "type": "string"
      },
      "timezone": {
        "type": "string"
      },
      "changeDetectingColumns": {
        "type": "array",
        "items": {
          "type": "string"
        }
```

```
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "serverlessAurora": {
          "type": "string",
          "enum": ["true", "false"]
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
```

```
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
connectionConfiguration	Configuration information for the endpoint for the data source.
repositoryEndpointMetadata	Required configuration information for connecting your data source. • dbType—The type of Java database you are using, whether `mysql`, `db2`, `postgresql` , `oracle`, or `sqlserver` . • dbHost—The database host name. • dbPort—The database port. • dbInstance—The database instance.
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings. Specify the type of data source and the secret ARN.
document	A list of objects that map the attributes or field names of your database content to Amazon Q index field names. For more information, see Fiel.
additionalProperties	Additional configuration options for your content in your data source. Use to include or

Configuration	Description
	exclude specific content in your database data source.
primaryKey	Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
titleColumn	Provide the name of the column in your database table that you want to designate as the column with document titles.
bodyColumn	Provide the name of the column in your database table that you want to designate as the column with document body text. Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.
sqlQuery	Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
timestampColumn	Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
timestampFormat	Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.

Configuration	Description
timezone	Enter the name of the column which contains time zones for the content to be crawled.
changeDetectingColumns	Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns
allowedUsersColumns	Enter the name of the column which contains User IDs to be allowed access to content.
allowedGroupsColumn	Enter the name of the column which contains User IDs to be allowed access to content.
sourceURIColumn	Enter the name of the column which contains Source URLs to be indexed.
isSslEnabled	`true` to add a path to an SSL certificate file stored in an Amazon S3 bucket.
type	The type of data source. Specify `JDBC` as your data source type.

Configuration	Description
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose • `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.
secretArn	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains username and password required to connect to your database. The secret must contain a JSON structure with the following keys: `{ "username": " database username", "password": " password" }`
version	The version of the template that is currently supported.

How Amazon Q Business connector crawls MySQL ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect a database data source to Amazon Q, Amazon Q crawls user and group information from a column in the source table. You specify this column in the console or using the `configuration` parameter as part of the `CreateDataSource` operation.

If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

A database data source has the following limitations:

- You can only specify an allow list for a database data source. You can't specify a deny list.
- You can only specify groups. You can't specify individual users for the allow list.
- The database column should be a string containing a semicolon delimited list of groups.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

MySQL data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional

document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q PostgreSQL connector supports the following field mappings:

Supported field mappings

- Document

Document

JDBC field name	Index field name	Description	Data type
jd_document_id	jd_document_id	Custom	String
jd_document_title	jd_document_title	Custom	String
jd_source_uri	_source_uri	Default	String

IAM role for MySQL connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
```

```
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Oracle Database to Amazon Q Business

> **Note**
>
> Oracle Database connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Oracle Database is a database management system. You can connect your Oracle Database instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

The Amazon Q Oracle Database data source connector supports Oracle Database 18c, 19c, and 21c.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials. Also, avoid adding tables with sensitive data or personal identifiable information (PII).

Topics

- Known limitations for the Oracle Database connector
- Oracle Database connector overview
- Prerequisites for connecting Amazon Q Business to Oracle Database
- Connecting Amazon Q Business to Oracle Database using the console
- Connecting Amazon Q Business to Oracle Database using APIs
- How Amazon Q Business connector crawls Oracle Database ACLs
- Amazon Q Business data source connector field mappings
- IAM role for Oracle Database connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Oracle Database connector

- Deleted database rows will not be tracked in when Amazon Q checks for updated content.
- The size of field names and values in a row of your database can't exceed 400KB.
- Column names should only contain alphanumeric characters and not spaces.
- If you have a large amount of data in your database data source, and do not want Amazon Q to index all your database content after the first sync, you can choose to sync only new, modified, or deleted documents.

Oracle Database connector overview

The following table gives an overview of the Amazon Q Oracle Database connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic
	Authentication credentials	• Username of database user • Password of database user
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Driver version	Oracle – 21.1.0.0
	Data source version	Oracle Database 18c, 19c, 21c
	Identity crawling	No
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Document **Note** Each database row is considered an individual searchable Amazon Q document. See What is a document? for more details on what each connector crawls as a document.

Category	Feature	Support
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Oracle Database

Before you begin, make sure that you have completed the following prerequisites.

In Oracle Database, make sure you have:

- Noted your database username and password.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials.

- Copied your database host URL, port, and instance.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Oracle Database authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Oracle Database using the console

The following procedure outlines how to connect Amazon Q to Oracle Database using the AWS Management Console.

Connecting Amazon Q to Oracle Database

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Oracle Database** data source to your Amazon Q application.
5. Then, on the **Oracle Database** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, enter the following information:

   a. **Host** – Enter the database host name.

   b. **Port** – Enter the database port.

   c. **Instance** – Enter the database instance.

   d. **Enable SSL certificate location** – Choose to enter the Amazon S3 path to your SSL certificate file.
8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs**

to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. In **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. For **Database username**, and **Password** – Enter the authentication credential values you copied from your database.

   c. Choose **Save**.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.

12. In **Sync scope**, enter the following information:

    - **SQL query** – Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
    - **Primary key column** – Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.

- **Title column** – Provide the name of the column in your database table that you want to designate as the column with document titles.
- **Body column** – Provide the name of the column in your database table that you want to designate as the column with document body text.

  Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

13. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Additional configuration – *optional*** – Configure the following settings:

    - **Change-detecting columns** – Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns.
    - **Users' IDs column** – Enter the name of the column which contains User IDs to be allowed access to content.
    - **Groups column** – Enter the name of the column that contains groups to be allowed access to content.
    - **Source URLs column** – Enter the name of the column which contains Source URLs to be indexed.
    - **Time stamps column** – Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
    - **Time zones column** – Enter the name of the column which contains time zones for the content to be crawled.
    - **Time stamps format** – Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.

15. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

- **Full sync** – Sync all content regardless of the previous sync status.
- **New or modified content sync** – Sync only new and modified documents.
- **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

For more details, see Sync mode.

16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
18. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Oracle Database using APIs

You use the `CreateDataSource` action to connect a data source to your Amazon Q application.

Then, you use the `configuration` parameter to provide a JSON schema with all other configuration information specific to your data source connector.

Oracle Database JSON schema

The following is the Oracle Database JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
```

```
            ]
          },
          "dbHost": {
            "type": "string"
          },
          "dbPort": {
            "type": "string"
          },
          "dbInstance": {
            "type": "string"
          }
        },
        "required": [
          "dbType",
          "dbHost",
          "dbPort",
          "dbInstance"
        ]
      }
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "document": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string"
                  },
                  "dataSourceFieldName": {
                    "type": "string"
```

```
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
      "timestampColumn": {
        "type": "string"
      },
      "timestampFormat": {
        "type": "string"
      },
      "timezone": {
```

```
          "type": "string"
        },
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "serverlessAurora": {
          "type": "string",
          "enum": ["true", "false"]
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
```

```
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
connectionConfiguration	Configuration information for the endpoint for the data source.
repositoryEndpointMetadata	Required configuration information for connecting your data source. • dbType—The type of Java database you are using, whether `mysql`, db2, `postgresql` , `oracle`, or `sqlserver` . • dbHost—The database host name. • dbPort—The database port. • dbInstance—The database instance.
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings. Specify the type of data source and the secret ARN.

Configuration	Description
document	A list of objects that map the attributes or field names of your database content to Amazon Q index field names. For more information, see Fiel.
additionalProperties	Additional configuration options for your content in your data source. Use to include or exclude specific content in your database data source.
primaryKey	Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
titleColumn	Provide the name of the column in your database table that you want to designate as the column with document titles.
bodyColumn	Provide the name of the column in your database table that you want to designate as the column with document body text. Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.
sqlQuery	Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.

Configuration	Description
timestampColumn	Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
timestampFormat	Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.
timezone	Enter the name of the column which contains time zones for the content to be crawled.
changeDetectingColumns	Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns
allowedUsersColumns	Enter the name of the column which contains User IDs to be allowed access to content.
allowedGroupsColumn	Enter the name of the column which contains User IDs to be allowed access to content.
sourceURIColumn	Enter the name of the column which contains Source URLs to be indexed.
isSslEnabled	`true` to add a path to an SSL certificate file stored in an Amazon S3 bucket.
type	The type of data source. Specify `JDBC` as your data source type.

Configuration	Description
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose • `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.
secretArn	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains username and password required to connect to your database. The secret must contain a JSON structure with the following keys: `{ "username": " database username", "password": " password" }`
version	The version of the template that is currently supported.

How Amazon Q Business connector crawls Oracle Database ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect a database data source to Amazon Q, Amazon Q crawls user and group information from a column in the source table. You specify this column in the console or using the `configuration` parameter as part of the `CreateDataSource` operation.

If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

A database data source has the following limitations:

- You can only specify an allow list for a database data source. You can't specify a deny list.
- You can only specify groups. You can't specify individual users for the allow list.
- The database column should be a string containing a semicolon delimited list of groups.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Amazon Q Business data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional

document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q PostgreSQL connector supports the following field mappings:

Supported field mappings

- Document

Document

JDBC field name	Index field name	Description	Data type
jd_document_id	jd_document_id	Custom	String
jd_document_title	jd_document_title	Custom	String
jd_source_uri	_source_uri	Default	String

IAM role for Oracle Database connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
```

```
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting PostgreSQL to Amazon Q Business

> **Note**
>
> PostgreSQL connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

PostgreSQL is an open source database management system. You can connect your PostgreSQL instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

The Amazon Q PostgreSQL data source connector supports PostgreSQL 9.6.

Important

As a best practice, provide Amazon Q with read-only database credentials. Also, avoid adding tables with sensitive data or personal identifiable information (PII).

Topics

- Known limitations for the PostgreSQL connector
- PostgreSQL connector overview
- Prerequisites for connecting Amazon Q Business to PostgreSQL
- Connecting Amazon Q Business to PostgreSQL using the console
- Connecting Amazon Q Business to PostgreSQL using APIs
- How Amazon Q Business connector crawls PostgreSQL ACLs
- PostgreSQL data source connector field mappings
- IAM role for PostgreSQL connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the PostgreSQL connector

- Deleted database rows will not be tracked in when Amazon Q checks for updated content.
- The size of field names and values in a row of your database can't exceed 400KB.
- Column names should only contain alphanumeric characters and not spaces.
- If you have a large amount of data in your database data source, and do not want Amazon Q to index all your database content after the first sync, you can choose to sync only new, modified, or deleted documents.

PostgreSQL connector overview

The following table gives an overview of the Amazon Q Business PostgreSQL connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic
	Authentication credentials	• Username of database user • Password of database user
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Driver version	PostgreSQL – 42.3.2
	Data source version	PostgreSQL 9.6
	Identity crawling	No
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Document **Note** Each database row is considered an individual searchable Amazon Q document. See What is a document? for more details on what each connector crawls as a document.

Category	Feature	Support
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to PostgreSQL

Before you begin, make sure that you have completed the following prerequisites.

In PostgreSQL, make sure you have:

- Noted your database username and password.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials.

- Copied your database host URL, port, and instance.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your PostgreSQL authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to PostgreSQL using the console

The following procedure outlines how to connect Amazon Q Business to PostgreSQL using the AWS Management Console.

Connecting Amazon Q to PostgreSQL

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **PostgreSQL** data source to your Amazon Q application.
5. Then, on the **PostgreSQL** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, enter the following information:

   a. **Host** – Enter the database host URL.

   b. **Port** – Enter the database port, for example, `5432`.

   c. **Instance** – Enter the database instance, for example `postgres`.

   d. **Enable SSL certificate location** – Choose to enter the Amazon S3 path to your SSL certificate file.
8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs**

to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. In **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. For **Database username**, and **Password** – Enter the authentication credential values you copied from your database.

   c. Choose **Save**.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.

12. In **Sync scope**, enter the following information:

    - **SQL query** – Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
    - **Primary key column** – Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.

- **Title column** – Provide the name of the column in your database table that you want to designate as the column with document titles.
- **Body column** – Provide the name of the column in your database table that you want to designate as the column with document body text.

  Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

13. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Additional configuration – *optional*** – Configure the following settings:

    - **Change-detecting columns** – Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns.
    - **Users' IDs column** – Enter the name of the column which contains User IDs to be allowed access to content.
    - **Groups column** – Enter the name of the column that contains groups to be allowed access to content.
    - **Source URLs column** – Enter the name of the column which contains Source URLs to be indexed.
    - **Time stamps column** – Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
    - **Time zones column** – Enter the name of the column which contains time zones for the content to be crawled.
    - **Time stamps format** – Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.

15. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

- **Full sync** – Sync all content regardless of the previous sync status.
- **New or modified content sync** – Sync only new and modified documents.
- **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

For more details, see Sync mode.

16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
18. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to PostgreSQL using APIs

You use the `CreateDataSource` action to connect a data source to your Amazon Q application.

Then, you use the `configuration` parameter to provide a JSON schema with all other configuration information specific to your data source connector.

PostgreSQL JSON schema

The following is the PostgreSQL JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
```

```
            ]
          },
          "dbHost": {
            "type": "string"
          },
          "dbPort": {
            "type": "string"
          },
          "dbInstance": {
            "type": "string"
          }
        },
        "required": [
          "dbType",
          "dbHost",
          "dbPort",
          "dbInstance"
        ]
      }
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "document": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string"
                  },
                  "dataSourceFieldName": {
                    "type": "string"
```

```
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
      "timestampColumn": {
        "type": "string"
      },
      "timestampFormat": {
        "type": "string"
      },
      "timezone": {
```

```
          "type": "string"
        },
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "serverlessAurora": {
          "type": "string",
          "enum": ["true", "false"]
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
```

```
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
connectionConfiguration	Configuration information for the endpoint for the data source.
repositoryEndpointMetadata	Required configuration information for connecting your data source. • dbType—The type of Java database you are using, whether `mysql`, db2, `postgresql` , `oracle`, or `sqlserver` . • dbHost—The database host name. • dbPort—The database port. • dbInstance—The database instance.
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings. Specify the type of data source and the secret ARN.

Configuration	Description
document	A list of objects that map the attributes or field names of your database content to Amazon Q index field names. For more information, see Fiel.
additionalProperties	Additional configuration options for your content in your data source. Use to include or exclude specific content in your database data source.
primaryKey	Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
titleColumn	Provide the name of the column in your database table that you want to designate as the column with document titles.
bodyColumn	Provide the name of the column in your database table that you want to designate as the column with document body text. Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.
sqlQuery	Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.

Configuration	Description
timestampColumn	Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
timestampFormat	Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.
timezone	Enter the name of the column which contains time zones for the content to be crawled.
changeDetectingColumns	Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns
allowedUsersColumns	Enter the name of the column which contains User IDs to be allowed access to content.
allowedGroupsColumn	Enter the name of the column which contains User IDs to be allowed access to content.
sourceURIColumn	Enter the name of the column which contains Source URLs to be indexed.
isSslEnabled	`true` to add a path to an SSL certificate file stored in an Amazon S3 bucket.
type	The type of data source. Specify `JDBC` as your data source type.

Configuration	Description
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose • `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.
secretArn	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains username and password required to connect to your database. The secret must contain a JSON structure with the following keys: `{ "username": " database username", "password": " password" }`
version	The version of the template that is currently supported.

How Amazon Q Business connector crawls PostgreSQL ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect a database data source to Amazon Q, Amazon Q crawls user and group information from a column in the source table. You specify this column in the console or using the `configuration` parameter as part of the `CreateDataSource` operation.

If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

A database data source has the following limitations:

- You can only specify an allow list for a database data source. You can't specify a deny list.
- You can only specify groups. You can't specify individual users for the allow list.
- The database column should be a string containing a semicolon delimited list of groups.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

PostgreSQL data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional

document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q PostgreSQL connector supports the following field mappings:

Supported field mappings

- Document

Document

JDBC field name	Index field name	Description	Data type
jd_document_id	jd_document_id	Custom	String
jd_document_title	jd_document_title	Custom	String
jd_source_uri	_source_uri	Default	String

IAM role for PostgreSQL connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
```

```
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Quip to Amazon Q Business

> **Note**
>
> Quip connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Quip is a collaborative productivity software that offers real time document-authoring capabilities. You can connect your Quip instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the Amazon Q Business Quip connector
- Quip connector overview
- Prerequisites for connecting Amazon Q Business to Quip
- Retrieving Quip credentials
- Connecting Amazon Q Business to Quip using the console
- Connecting Amazon Q Business to Quip using APIs
- How Amazon Q Business connector crawls Quip ACLs
- Quip data source connector field mappings
- IAM role for Amazon Q Business Quip connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Amazon Q Business Quip connector

The Quip connector has the following known limitations:

- Only **Full sync** is supported by default. For **New, modified, or deleted content sync**, Admin API access is required and Admin API has to be enabled on the Quip website .
- Only data in shared folders will be crawled by the Amazon Q Quip connector. Private folders, other than the private folders belonging to the Private Access Token user, will not be crawled.
- Quip doesn't store file types and file paths. Amazon Q Quip connector can't support inclusion and exclusion filters on these.

Quip connector overview

The following table gives an overview of the Quip connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Personal Access Token
	Authentication credentials	Quip token
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	No. Quip doesn't have the concept of user groups.
	VPC	Yes
Crawl features	**Custom metadata**	No
	Entities	Yes. The following entities are supported: • Thread • Message • Attachment See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports default field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Crawl file comments • Crawl chat rooms • Crawl attachments
	Sync mode	Supports full and incremental (new, modified, and deleted) sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Quip

Before you begin, make sure that you have completed the following prerequisites.

In Quip, make sure you have:

- A Quip account with administrative permissions.
- Created Quip authentication credentials that include a personal access token. See Quip documentation on authentication for more information.
- Copied your Quip site domain. For example, *`https://quip-company.quipdomain.com/browse`* where *`quipdomain`* is the domain.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Quip authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Retrieving Quip credentials

Before you connect Quip to Amazon Q, you need to create and retrieve the Quip credentials you will use to connect Quip to Amazon Q.

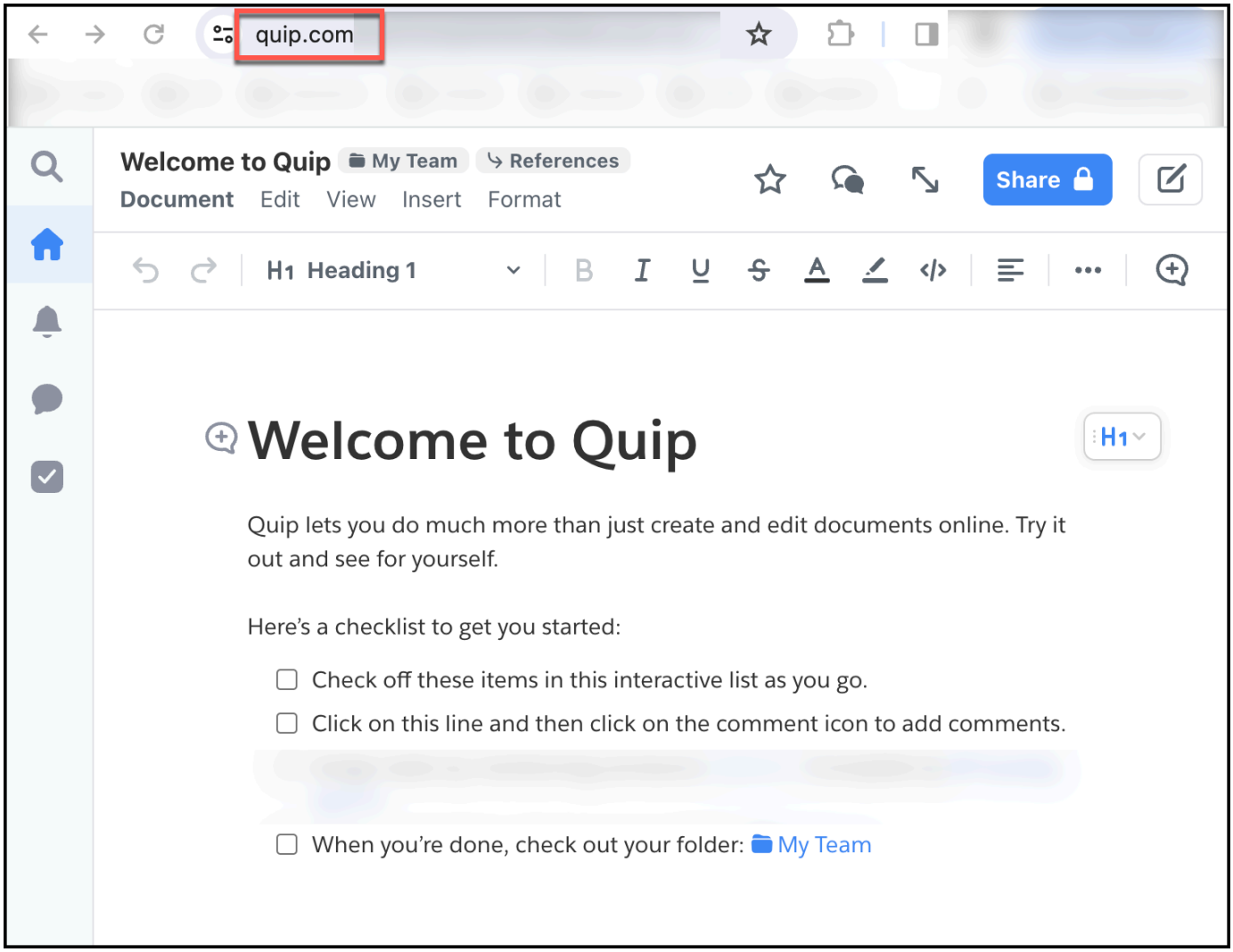
The following procedure gives you an overview of how to configure Quip for connecting with Amazon Q by creating a API access token.

Configuring Quip authentication for Amazon Q

1. Log in to your Quip account using a web browser of your choice and sign into your Quip workspace.

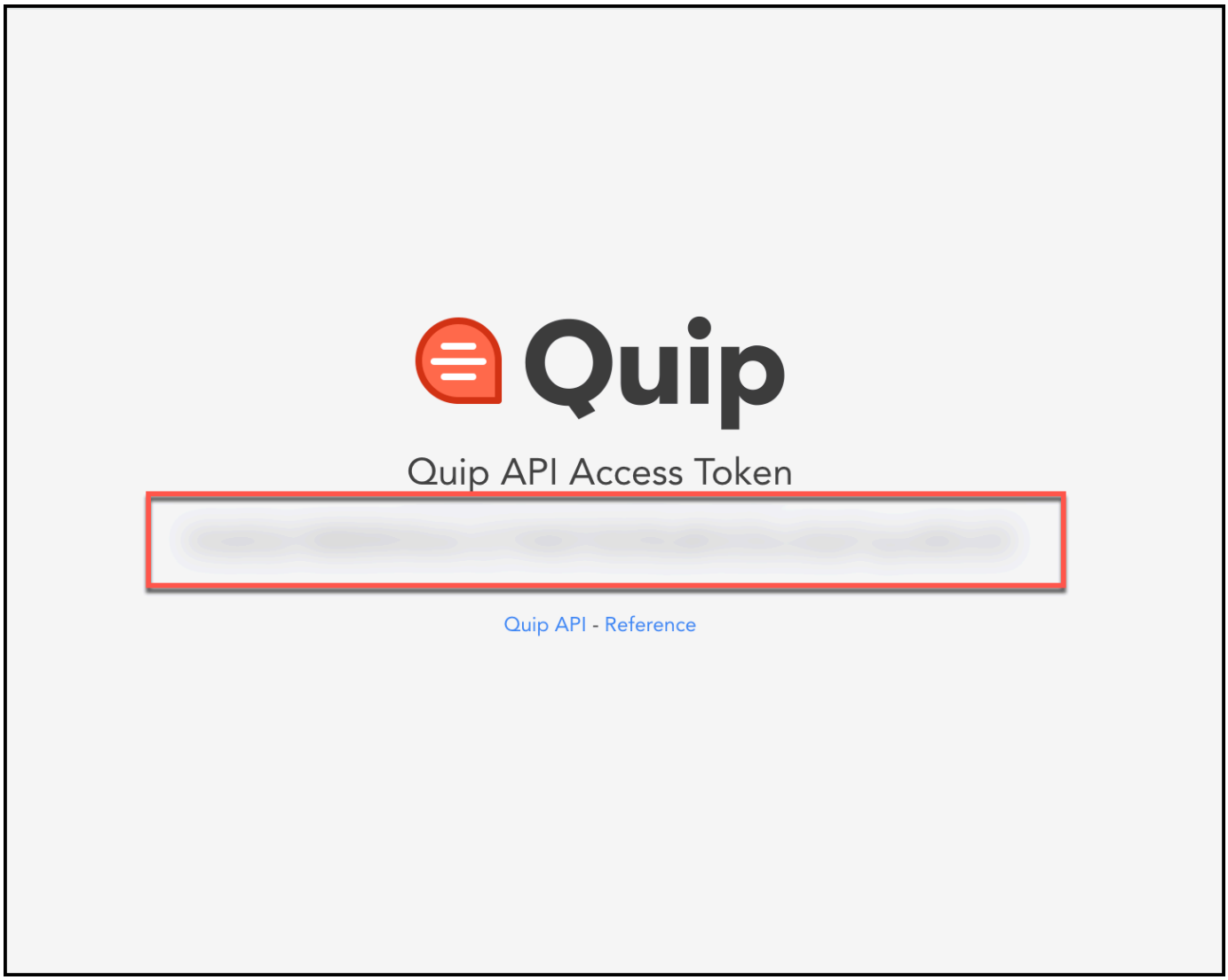
> **Note**
>
> To configure Quip for Amazon Q, you must be an admin user in the Quip account.

2. From the browser URL, note your Quip domain name. You will need this both to connect to Amazon Q and also to generate an API access token.



3. In a text editor of your choice, copy and paste the following: `https://domain/dev/token`. Then, replace *`domain`* with the Quip domain you copied in the last step. Copy the URL.

4. Open a new browser window and paste the formatted URL you created in the last step. Quip will return an API access token in your browser window.



You now have the Quip domain name and Quip API access token you need to connect to Amazon Q.

Connecting Amazon Q Business to Quip using the console

The following procedure outlines how to connect Amazon Q Business to Quip using the AWS Management Console.

Connecting Amazon Q to Quip

1. Sign in to the AWS Management Console and open the Amazon Q Business console.

2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Quip** data source to your Amazon Q application.
5. Then, on the **Quip** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. **Source** – Enter your **Quip domain name**. You can find your domain name in the browser URL of your Quip. For example, *`https://quip-company.quipdomain.com/browse`*, the domain is "quipdomain".
8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
9. **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. **Quip token** – Enter the Quip personal access token you created in your Quip account.
10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

12. In **Sync scope**, enter the following information:

    a. **Add Quip folder IDs to crawl** – Enter the Quip folder IDs you want to crawl. You can find your folder ID in the browser URL when you access your folder in Quip. For example, *`https://quip-company.quipdomain.com/zlLuOVNSarTL/folder-name`*, the folder ID is "zlLuOVNSarTL"..

> **Note**
>
> To crawl a root folder, including all sub-folders and documents inside it, input the root folder ID. To crawl specific sub-folders, add the specific sub-folder IDs.

    b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

    c. (Optional) **Additional configuration – *optional*** – Configure the following settings:

- **Content types** – Choose between crawling **All content**, **File comments**, **Chat rooms** and **Attachments**.
- **Regex patterns** – Add regex patterns to include or exclude file names, file types, or file paths. You can have a total of 100 patterns.

    d. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete

phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

13. For **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

14. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.

15. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.

16. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

    For more information, see Field mappings.

17. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Quip using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Quip JSON schema

The following is the Quip JSON schema:

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "type": "object",
    "properties": {
        "connectionConfiguration": {
            "type": "object",
            "properties": {
                "repositoryEndpointMetadata": {
                    "type": "object",
                    "properties": {
                        "domain": {
                            "type": "string"
                        }
                    },
```

```
                "required": [
                    "domain"
                ]
            }
        },
        "required": [
            "repositoryEndpointMetadata"
        ]
    },
    "repositoryConfigurations": {
        "type": "object",
        "properties": {
            "thread": {
                "type": "object",
                "properties": {
                    "fieldMappings": {
                        "type": "array",
                        "items": [
                            {
                                "type": "object",
                                "properties": {
                                    "indexFieldName": {
                                        "type": "string"
                                    },
                                    "indexFieldType": {
                                        "type": "string",
                                        "enum": [
                                            "STRING",
                                            "STRING_LIST",
                                            "DATE"
                                        ]
                                    },
                                    "dataSourceFieldName": {
                                        "type": "string"
                                    },
                                    "dateFieldFormat": {
                                        "type": "string",
                                        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                                    }
                                },
                                "required": [
                                    "indexFieldName",
                                    "indexFieldType",
                                    "dataSourceFieldName"
```

```
                                ]
                            }
                        ]
                    }
                },
                "required": [
                    "fieldMappings"
                ]
            },
            "message": {
                "type": "object",
                "properties": {
                    "fieldMappings": {
                        "type": "array",
                        "items": [
                            {
                                "type": "object",
                                "properties": {
                                    "indexFieldName": {
                                        "type": "string"
                                    },
                                    "indexFieldType": {
                                        "type": "string",
                                        "enum": [
                                            "STRING",
                                            "STRING_LIST",
                                            "DATE"
                                        ]
                                    },
                                    "dataSourceFieldName": {
                                        "type": "string"
                                    },
                                    "dateFieldFormat": {
                                        "type": "string",
                                        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                                    }
                                },
                                "required": [
                                    "indexFieldName",
                                    "indexFieldType",
                                    "dataSourceFieldName"
                                ]
                            }
                        ]
```

```
                    }
                },
                "required": [
                    "fieldMappings"
                ]
            },
            "attachment": {
                "type": "object",
                "properties": {
                    "fieldMappings": {
                        "type": "array",
                        "items": [
                            {
                                "type": "object",
                                "properties": {
                                    "indexFieldName": {
                                        "type": "string"
                                    },
                                    "indexFieldType": {
                                        "type": "string",
                                        "enum": [
                                            "STRING",
                                            "STRING_LIST",
                                            "DATE"
                                        ]
                                    },
                                    "dataSourceFieldName": {
                                        "type": "string"
                                    },
                                    "dateFieldFormat": {
                                        "type": "string",
                                        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                                    }
                                },
                                "required": [
                                    "indexFieldName",
                                    "indexFieldType",
                                    "dataSourceFieldName"
                                ]
                            }
                        ]
                    }
                },
                "required": [
```

```
                    "fieldMappings"
                ]
            }
        }
    },
    "additionalProperties": {
        "type": "object",
        "properties": {
            "isCrawlAcl": {
                "type": "boolean"
            },
            "maxFileSizeInMegaBytes": {
                "type": "string"
            },
            "fieldForUserId": {
                "type": "string"
            },
            "folderIds": {
                "type": "array",
                "items": {
                    "type": "string"
                }
            },
            "crawlFileComments": {
                "type": "boolean"
            },
            "crawlChatRooms": {
                "type": "boolean"
            },
            "crawlAttachments": {
                "type": "boolean"
            },
            "inclusionPatterns": {
                "type": "array",
                "items": {
                    "type": "string"
                }
            },
            "exclusionPatterns": {
                "type": "array",
                "items": {
                    "type": "string"
                }
            }
```

```
            },
            "required": []
        },
        "type": {
            "type": "string",
            "pattern": "QUIP"
        },
        "syncMode": {
            "type": "string",
            "enum": [
                "FULL_CRAWL",
                "FORCED_FULL_CRAWL"
            ]
        },
        "secretArn": {
            "type": "string",
            "minLength": 20,
            "maxLength": 2048
        }
    },
    "version": {
        "type": "string",
        "anyOf": [
            {
                "pattern": "1.0.0"
            }
        ]
    },
    "required": [
        "connectionConfiguration",
        "repositoryConfigurations",
        "syncMode",
        "additionalProperties",
        "secretArn",
        "type"
    ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the endpoint for the data source.
`repositoryEndpointMetadata`	The endpoint information for the data source.
`domain`	Your Quip site domain. For example, *`https://quip-company.quipdomain.com/browse`* where *`quipdomain`* is the domain.
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.
• `thread` • `message` • `attachment`	A list of objects that map the attributes or field names of your Quip pages and assets to Amazon Q index field names.
`additionalProperties`	Additional configuration options for your content in your data source.
`isCrawlAcl`	Specify `true` to crawl access control informati on from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit

Configuration	Description
	you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.
`folderIds`	Specify folder IDs to crawl.
• `crawlFileComments` • `crawlChatRooms` • `crawlAttachments`	`true` to index.
• `inclusionPatterns`	A list of regular expression patterns to include specific content in your Quip data source. Content that matches the patterns are included in the index. Content that doesn't match the pattern are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.
• `exclusionPatterns`	A list of regular expression patterns to exclude specific content in your Quip data source. Content that matches the patterns are excluded from the index. Content that doesn't match the patterns are included in the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.
`type`	The type of data source. Specify `QUIP` as your data source type.

Configuration	Description
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/principal informati on on users and groups with access to specific documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index.

Configuration	Description
`secretArn`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Quip. The secret must contain a JSON structure with the following keys: `{ "accessToken": " token" }`
`version`	The version of this template that's currently supported.

How Amazon Q Business connector crawls Quip ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an Quip data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your Quip instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

The Quip user IDs are mapped as follows:

- `_user_id`—User IDs exist in Quip on files where there are set access permissions. They are mapped from the user emails as the IDs in Quip.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Quip data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Quip connector supports the following entities and the associated reserved and custom attributes.

> **Note**
>
> You can map any Quip field to the document title or document body Amazon Q reserved/default index fields.

Supported entities and field mappings

- Thread

- Message
- Attachment

Thread

Amazon Q supports crawling Quip Threads and offers the following thread field mappings.

Quip field name	Index field name	Description	Data type
qp_authors	_authors	Default	String list
qp_category	_category	Default	String
qp_file_type	qp_file_type	Custom	String
qp_document_title	qp_document_title	Custom	String
qp_source_uri	_source_uri	Default	String
qp_created_at	_created_at	Default	Date
qp_updated_at	_last_updated_at	Default	Date

Message

Amazon Q supports crawling Quip Messages and offers the following message field mappings.

Quip field name	Index field name	Description	Data type
qp_authors	_authors	Default	String list
qp_category	_category	Default	String
qp_source_uri	_source_uri	Default	String
qp_parent_file	qp_parent_file	Custom	String
qp_created_at	_created_at	Default	Date
qp_updated_at	_last_updated_at	Default	Date

Attachment

Amazon Q supports crawling Quip attachments and offers the following attachment field mappings.

Quip field name	Index field name	Description	Data type
qp_authors	_authors	Default	String list
qp_category	_category	Default	String
qp_source_uri	_source_uri	Default	String
qp_file_type	qp_file_type	Custom	String
qp_parent_file	qp_parent_file	Custom	String
qp_blob_id	qp_blob_id	Custom	String
qp_created_at	_created_at	Default	Date
qp_updated_at	_last_updated_at	Default	Date

IAM role for Amazon Q Business Quip connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.

- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
```

```
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
```

```
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Amazon RDS (Microsoft SQL Server) to Amazon Q Business

> **Note**
>
> Amazon RDS (Microsoft SQL Server) connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Amazon RDS (Microsoft SQL Server) is a relational database management system (RDBMS) built for the cloud. You can connect your Amazon RDS (Microsoft SQL Server) instance to Amazon Q Business – using either the AWS Management Console, CLI, or the CreateDataSource API – and create an Amazon Q web experience.

The Amazon Q Microsoft SQL Server data source connector supports MS SQL Server 2019.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials. Also, avoid adding tables with sensitive data or personal identifiable information (PII).

Topics

- Known limitations for the Amazon RDS (Microsoft SQL Server) connector
- Amazon RDS (Microsoft SQL Server) connector overview
- Prerequisites for connecting Amazon Q Business to Amazon RDS (Microsoft SQL Server)
- Connecting Amazon Q Business to Amazon RDS (Microsoft SQL Server) using the console
- Connecting Amazon Q Business to Amazon RDS (Microsoft SQL Server) using APIs
- How Amazon Q Business connector crawls Amazon RDS (Microsoft SQL Server) ACLs
- Amazon RDS (Microsoft SQL Server) data source connector field mappings
- IAM role for Amazon RDS (Microsoft SQL Server) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Amazon RDS (Microsoft SQL Server) connector

- Deleted database rows will not be tracked in when Amazon Q checks for updated content.
- The size of field names and values in a row of your database can't exceed 400KB.
- Column names should only contain alphanumeric characters and not spaces.
- If you have a large amount of data in your database data source, and do not want Amazon Q to index all your database content after the first sync, you can choose to sync only new, modified, or deleted documents.

Amazon RDS (Microsoft SQL Server) connector overview

The following table gives an overview of the Amazon Q Business Amazon RDS (Microsoft SQL Server) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic
	Authentication credentials	• Username of database user • Password of database user
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Driver version	Microsoft SQL Server – 10.2.0.jre11
	Data source version	Microsoft SQL Server 2019

Category	Feature	Support
	Identity crawling	No
	VPC	Yes
Crawl features	Custom metadata	Yes
	Entities	Yes. The following entities are supported: • Document **Note** Each database row is considered an individual searchable Amazon Q document. See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Amazon RDS (Microsoft SQL Server)

Before you begin, make sure that you have completed the following prerequisites.

In Amazon RDS (Microsoft SQL Server), make sure you have:

- Noted your database username and password.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials.

- Copied your database host URL, port, and instance.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Amazon RDS (Microsoft SQL Server) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Amazon RDS (Microsoft SQL Server) using the console

On the **Amazon RDS (Microsoft SQL Server)** page, enter the following information:

1. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

   > **Note**
   >
   > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

2. In **Source**, enter the following information:

   a. **Host** – Enter the database host name.

   b. **Port** – Enter the database port.

   c. **Instance** – Enter the database instance.

   d. **SSL certificate location** – Choose to enter the Amazon S3 path to your SSL certificate file.

3. In **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. For **Database username**, and **Password** – Enter the authentication credential values you copied from your database.

   c. Choose **Save**.

4. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

   a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

   b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

   For more information, see VPC.

5. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

   > **Note**
   >
   > Creating a new service IAM role is recommended.

   For more information, see IAM role.

6. In **Sync scope**, enter the following information:

- **SQL query** – Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
- **Primary key column** – Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
- **Title column** – Provide the name of the column in your database table that you want to designate as the column with document titles.
- **Body column** – Provide the name of the column in your database table that you want to designate as the column with document body text.

  Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

7. **Advanced settings**

   Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

8. In **Additional configuration – *optional*** – Configure the following settings:

   - **Change-detecting columns** – Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns.
   - **Users' IDs column** – Enter the name of the column which contains User IDs to be allowed access to content.
   - **Groups column** – Enter the name of the column that contains groups to be allowed access to content.
   - **Source URLs column** – Enter the name of the column which contains Source URLs to be indexed.
   - **Time stamps column** – Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.

- **Time zones column** – Enter the name of the column which contains time zones for the content to be crawled.
- **Time stamps format** – Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.

9. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

   - **Full sync** – Sync all content regardless of the previous sync status.
   - **New or modified content sync** – Sync only new and modified documents.
   - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

   For more details, see Sync mode.

10. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
11. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
12. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

13. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Amazon RDS (Microsoft SQL Server) using APIs

You use the `CreateDataSource` action to connect a data source to your Amazon Q Business application.

Then, you use the `configuration` parameter to provide a JSON schema with all other configuration information specific to your data source connector.

Amazon RDS (Microsoft SQL Server) JSON schema

The following is the Amazon RDS (Microsoft SQL Server) JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
```

```
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            },
            "dbInstance": {
              "type": "string"
            }
          },
          "required": [
            "dbType",
            "dbHost",
            "dbPort",
            "dbInstance"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "document": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
```

```
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string"
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
```

```
        },
        "timestampColumn": {
          "type": "string"
        },
        "timestampFormat": {
          "type": "string"
        },
        "timezone": {
          "type": "string"
        },
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "serverlessAurora": {
          "type": "string",
          "enum": ["true", "false"]
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL"
      ]
    },
    "secretArn": {
```

```
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
connectionConfiguration	Configuration information for the endpoint for the data source.
repositoryEndpointMetadata	Required configuration information for connecting your data source. • dbType—The type of Java database you are using, whether `mysql`, db2, `postgresql` , `oracle`, or `sqlserver` . • dbHost—The database host name. • dbPort—The database port. • dbInstance—The database instance.
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring

Configuration	Description
	specific types of content and field mappings. Specify the type of data source and the secret ARN.
document	A list of objects that map the attributes or field names of your database content to Amazon Q index field names. For more information, see Mapping data source fields.
additionalProperties	Additional configuration options for your content in your data source. Use to include or exclude specific content in your database data source.
primaryKey	Provide the primary key for the database table. This identifies a table within your database.
titleColumn	Provide the name of the document title column within your database table.
bodyColumn	Provide the name of the document title column within your database table.
sqlQuery	Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query. If a table name has special characters, put it in square brackets "[ ]" in the SQL query. For example: `select * from [my-database-table] .`

Configuration	Description
timestampColumn	Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
timestampFormat	Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.
timezone	Enter the name of the column which contains time zones for the content to be crawled.
changeDetectingColumns	Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns
allowedUsersColumns	Enter the name of the column which contains User IDs to be allowed access to content.
allowedGroupsColumn	Enter the name of the column which contains User IDs to be allowed access to content.
sourceURIColumn	Enter the name of the column which contains Source URLs to be indexed.
isSslEnabled	`true` to add a path to an SSL certificate file stored in an Amazon S3 bucket.
type	The type of data source. Specify `JDBC` as your data source type.

Configuration	Description
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose • `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.
secretArn	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains user name and password required to connect to your database. The secret must contain a JSON structure with the following keys: `{ "username": " database username", "password": " password" }`
version	The version of the template that is currently supported.

How Amazon Q Business connector crawls Amazon RDS (Microsoft SQL Server) ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect a database data source to Amazon Q, Amazon Q crawls user and group information from a column in the source table. You specify this column in the console or using the `configuration` parameter as part of the `CreateDataSource` operation.

If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

A database data source has the following limitations:

- You can only specify an allow list for a database data source. You can't specify a deny list.
- You can only specify groups. You can't specify individual users for the allow list.
- The database column should be a string containing a semicolon delimited list of groups.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Amazon RDS (Microsoft SQL Server) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional

document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q PostgreSQL connector supports the following field mappings:

Supported field mappings

- Document

Document

JDBC field name	Index field name	Description	Data type
jd_document_id	jd_document_id	Custom	String
jd_document_title	jd_document_title	Custom	String
jd_source_uri	_source_uri	Default	String

IAM role for Amazon RDS (Microsoft SQL Server) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
```

```
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Amazon RDS (MySQL) to Amazon Q Business

> **Note**
>
> Amazon RDS (MySQL) connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Amazon RDS (MySQL) (Amazon Relational Database Service) is a web service that makes it easier to set up, operate, and scale a relational database in the AWS Cloud. You can connect your Amazon RDS (MySQL) instance to Amazon Q Business – using either the AWS Management Console, CLI, or the CreateDataSource API – and create an Amazon Q web experience.

The Amazon Q Aurora (MySQL) data source connector supports Amazon RDS MySql 5.6, 5.7, and 8.0.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials. Also, avoid adding tables with sensitive data or personal identifiable information (PII).

Topics

- Known limitations for the Amazon RDS (MySQL) connector
- Amazon RDS (MySQL) connector overview
- Prerequisites for connecting Amazon Q Business to Amazon RDS (MySQL)
- Connecting Amazon Q Business to Amazon RDS (MySQL) using the console
- Connecting Amazon Q Business to Amazon RDS (MySQL) using APIs
- How Amazon Q Business connector crawls Amazon RDS (MySQL) ACLs
- Amazon RDS (MySQL) data source connector field mappings
- IAM role for Amazon RDS (MySQL) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Amazon RDS (MySQL) connector

The Amazon RDS (MySQL) connector has the following known limitations:

- Deleted database rows will not be tracked in when Amazon Q checks for updated content.
- The size of field names and values in a row of your database can't exceed 400KB.

- Column names should only contain alphanumeric characters and not spaces.
- If you have a large amount of data in your database data source, and do not want Amazon Q to index all your database content after the first sync, you can choose to sync only new, modified, or deleted documents.

Amazon RDS (MySQL) connector overview

The following table gives an overview of the Amazon Q Business Amazon RDS (MySQL) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic
	Authentication credentials	• Username of database user • Password of database user
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Driver version	MySQL – 8.0.27
	Data source version	MySQL 5.6, 5.7, 8.0
	Identity crawling	No
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Document **Note** Each database row is considered an individual searchable Amazon Q document.

Category	Feature	Support
		See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Amazon RDS (MySQL)

Before you begin, make sure that you have completed the following prerequisites.

In Amazon RDS (MySQL), make sure you have:

- Noted your database username and password.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials.

- Copied your database host URL, port, and instance. You can find this information on the Amazon RDS console.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Amazon RDS (MySQL) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Amazon RDS (MySQL) using the console

The following procedure outlines how to connect Amazon Q Business to Amazon RDS (MySQL) using the AWS Management Console.

Connecting Amazon Q to Amazon RDS (MySQL)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Amazon RDS (MySQL)** data source to your Amazon Q application.
5. Then, on the **Amazon RDS (MySQL)** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, enter the following information:

   a. **Host** – Enter the database host URL, for example: `http://instance URL.region.rds.amazonaws.com`.

b. **Port** – Enter the database port, for example, `3306`.

c. **Instance** – Enter the database instance, for example `mysql`.

d. **SSL certificate location** – Choose to enter the Amazon S3 path to your SSL certificate file.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. In **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. For **Database username**, and **Password** – Enter the authentication credential values you copied from your database.

   c. Choose **Save**.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

    For more information, see IAM role.

12. In **Sync scope**, enter the following information:

- **SQL query** – Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
- **Primary key column** – Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
- **Title column** – Provide the name of the column in your database table that you want to designate as the column with document titles.
- **Body column** – Provide the name of the column in your database table that you want to designate as the column with document body text.

  Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

13. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Additional configuration – *optional*** – Configure the following settings:

    - **Change-detecting columns** – Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns.
    - **Users' IDs column** – Enter the name of the column which contains User IDs to be allowed access to content.
    - **Groups column** – Enter the name of the column that contains groups to be allowed access to content.
    - **Source URLs column** – Enter the name of the column which contains Source URLs to be indexed.
    - **Time stamps column** – Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.

- **Time zones column** – Enter the name of the column which contains time zones for the content to be crawled.
- **Time stamps format** – Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.

15. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New or modified content sync** – Sync only new and modified documents.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

    For more details, see Sync mode.

16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
18. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Amazon RDS (MySQL) using APIs

You use the `CreateDataSource` action to connect a data source to your Amazon Q application.

Then, you use the `configuration` parameter to provide a JSON schema with all other configuration information specific to your data source connector.

Amazon RDS (MySQL) JSON schema

The following is the Amazon RDS (MySQL) JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
```

```
            "type": "string",
            "enum": [
              "mysql",
              "db2",
              "postgresql",
              "oracle",
              "sqlserver"
            ]
          },
          "dbHost": {
            "type": "string"
          },
          "dbPort": {
            "type": "string"
          },
          "dbInstance": {
            "type": "string"
          }
        },
        "required": [
          "dbType",
          "dbHost",
          "dbPort",
          "dbInstance"
        ]
      }
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "document": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string"
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
```

```
        "timestampColumn": {
          "type": "string"
        },
        "timestampFormat": {
          "type": "string"
        },
        "timezone": {
          "type": "string"
        },
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "serverlessAurora": {
          "type": "string",
          "enum": ["true", "false"]
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
```

```
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
connectionConfiguration	Configuration information for the endpoint for the data source.
repositoryEndpointMetadata	Required configuration information for connecting your data source. • dbType—The type of Java database you are using, whether `mysql`, db2, `postgresql` , `oracle`, or `sqlserver` . • dbHost—The database host name. • dbPort—The database port. • dbInstance—The database instance.

Configuration	Description
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings. Specify the type of data source and the secret ARN.
document	A list of objects that map the attributes or field names of your database content to Amazon Q index field names. For more information, see Fiel.
additionalProperties	Additional configuration options for your content in your data source. Use to include or exclude specific content in your database data source.
primaryKey	Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
titleColumn	Provide the name of the column in your database table that you want to designate as the column with document titles.
bodyColumn	Provide the name of the column in your database table that you want to designate as the column with document body text. Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

Configuration	Description
sqlQuery	Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
timestampColumn	Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
timestampFormat	Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.
timezone	Enter the name of the column which contains time zones for the content to be crawled.
changeDetectingColumns	Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns
allowedUsersColumns	Enter the name of the column which contains User IDs to be allowed access to content.
allowedGroupsColumn	Enter the name of the column which contains User IDs to be allowed access to content.
sourceURIColumn	Enter the name of the column which contains Source URLs to be indexed.
isSslEnabled	`true` to add a path to an SSL certificate file stored in an Amazon S3 bucket.
type	The type of data source. Specify `JDBC` as your data source type.

Configuration	Description
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose • `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.
secretArn	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains username and password required to connect to your database. The secret must contain a JSON structure with the following keys: `{ "username": " database username", "password": " password" }`
version	The version of the template that is currently supported.

How Amazon Q Business connector crawls Amazon RDS (MySQL) ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect a database data source to Amazon Q, Amazon Q crawls user and group information from a column in the source table. You specify this column in the console or using the `configuration` parameter as part of the `CreateDataSource` operation.

If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

A database data source has the following limitations:

- You can only specify an allow list for a database data source. You can't specify a deny list.
- You can only specify groups. You can't specify individual users for the allow list.
- The database column should be a string containing a semicolon delimited list of groups.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Amazon RDS (MySQL) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional

document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q PostgreSQL connector supports the following field mappings:

Supported field mappings

- Document

Document

JDBC field name	Index field name	Description	Data type
jd_document_id	jd_document_id	Custom	String
jd_document_title	jd_document_title	Custom	String
jd_source_uri	_source_uri	Default	String

IAM role for Amazon RDS (MySQL) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
```

```
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Amazon RDS (Oracle) to Amazon Q Business

> **Note**
>
> Amazon RDS (Oracle) connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Amazon RDS (Oracle) (Amazon Relational Database Service) is a web service that makes it easier to set up, operate, and scale a relational database in the AWS Cloud. You can connect your Amazon RDS (Oracle) instance to Amazon Q Business – using either the AWS Management Console, CLI, or the CreateDataSource API – and create an Amazon Q web experience.

The Amazon RDS (Oracle) (Amazon Relational Database Service) data source connector supports Amazon RDS Oracle Database 21c, Oracle Database 19c, Oracle Database 12c.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials. Also, avoid adding tables with sensitive data or personal identifiable information (PII).

Topics

- Known limitations for the Amazon RDS (Oracle) connector
- Amazon RDS (Oracle) connector overview
- Prerequisites for connecting Amazon Q Business to Amazon RDS (Oracle)
- Connecting Amazon Q Business to Amazon RDS (Oracle) using the console
- Connecting Amazon Q Business to Amazon RDS (Oracle) using APIs
- How Amazon Q Business connector crawls Amazon RDS (Oracle) ACLs
- Amazon RDS (Oracle) data source connector field mappings
- IAM role for Amazon RDS (Oracle) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Amazon RDS (Oracle) connector

The Amazon RDS (Oracle) connector has the following known limitations:

- Deleted database rows will not be tracked in when Amazon Q checks for updated content.
- The size of field names and values in a row of your database can't exceed 400KB.

- Column names should only contain alphanumeric characters and not spaces.
- If you have a large amount of data in your database data source, and do not want Amazon Q to index all your database content after the first sync, you can choose to sync only new, modified, or deleted documents.

Amazon RDS (Oracle) connector overview

The following table gives an overview of the Amazon Q Business Amazon RDS (Oracle) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic
	Authentication credentials	• Username of database user • Password of database user
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Driver version	Oracle – 21.1.0.0
	Data source version	Oracle Database 12c, 19c, 21c
	Identity crawling	No
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Document **Note** Each database row is considered an individual searchable Amazon Q document.

Category	Feature	Support
		See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Amazon RDS (Oracle)

Before you begin, make sure that you have completed the following prerequisites.

In Amazon RDS (Oracle), make sure you have:

- Noted your database username and password.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials.

- Copied your database host URL, port, and instance.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Amazon RDS (Oracle) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Amazon RDS (Oracle) using the console

The following procedure outlines how to connect Amazon Q Business to Amazon RDS (Oracle) using the AWS Management Console.

Connecting Amazon Q to Amazon RDS (Oracle)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Amazon RDS (Oracle)** data source to your Amazon Q application.
5. Then, on the **Amazon RDS (Oracle)** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. **Source**, enter the following information:

   a. **Host** – Enter the database host name.

   b. **Port** – Enter the database port.

c. **Instance** – Enter the database instance.

d. **SSL certificate location** – Choose to enter the Amazon S3 path to your SSL certificate file.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. In **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. For **Database username**, and **Password** – Enter the authentication credential values you copied from your database.

   c. Choose **Save**.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.

12. In **Sync scope**, enter the following information:

- **SQL query** – Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
- **Primary key column** – Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
- **Title column** – Provide the name of the column in your database table that you want to designate as the column with document titles.
- **Body column** – Provide the name of the column in your database table that you want to designate as the column with document body text.

  Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

13. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Additional configuration – *optional*** – Configure the following settings:

    - **Change-detecting columns** – Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns.
    - **Users' IDs column** – Enter the name of the column which contains User IDs to be allowed access to content.
    - **Groups column** – Enter the name of the column that contains groups to be allowed access to content.
    - **Source URLs column** – Enter the name of the column which contains Source URLs to be indexed.
    - **Time stamps column** – Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.

- **Time zones column** – Enter the name of the column which contains time zones for the content to be crawled.
- **Time stamps format** – Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.

15. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New or modified content sync** – Sync only new and modified documents.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

    For more details, see Sync mode.

16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
18. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Amazon RDS (Oracle) using APIs

You use the `CreateDataSource` action to connect a data source to your Amazon Q application.

Then, you use the `configuration` parameter to provide a JSON schema with all other configuration information specific to your data source connector.

Amazon RDS (Oracle) JSON schema

The following is the Amazon RDS (Oracle) JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
```

```
            "type": "string",
            "enum": [
              "mysql",
              "db2",
              "postgresql",
              "oracle",
              "sqlserver"
            ]
          },
          "dbHost": {
            "type": "string"
          },
          "dbPort": {
            "type": "string"
          },
          "dbInstance": {
            "type": "string"
          }
        },
        "required": [
          "dbType",
          "dbHost",
          "dbPort",
          "dbInstance"
        ]
      }
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "document": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string"
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
```

```
        "timestampColumn": {
          "type": "string"
        },
        "timestampFormat": {
          "type": "string"
        },
        "timezone": {
          "type": "string"
        },
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "serverlessAurora": {
          "type": "string",
          "enum": ["true", "false"]
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
```

```
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
connectionConfiguration	Configuration information for the endpoint for the data source.
repositoryEndpointMetadata	Required configuration information for connecting your data source. • dbType—The type of Java database you are using, whether `mysql`, db2, `postgresql` , `oracle`, or `sqlserver` . • dbHost—The database host name. • dbPort—The database port. • dbInstance—The database instance.

Configuration	Description
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings. Specify the type of data source and the secret ARN.
document	A list of objects that map the attributes or field names of your database content to Amazon Q index field names. For more information, see Fiel.
additionalProperties	Additional configuration options for your content in your data source. Use to include or exclude specific content in your database data source.
primaryKey	Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
titleColumn	Provide the name of the column in your database table that you want to designate as the column with document titles.
bodyColumn	Provide the name of the column in your database table that you want to designate as the column with document body text. Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

Configuration	Description
sqlQuery	Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
timestampColumn	Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
timestampFormat	Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.
timezone	Enter the name of the column which contains time zones for the content to be crawled.
changeDetectingColumns	Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns
allowedUsersColumns	Enter the name of the column which contains User IDs to be allowed access to content.
allowedGroupsColumn	Enter the name of the column which contains User IDs to be allowed access to content.
sourceURIColumn	Enter the name of the column which contains Source URLs to be indexed.
isSslEnabled	`true` to add a path to an SSL certificate file stored in an Amazon S3 bucket.
type	The type of data source. Specify `JDBC` as your data source type.

Configuration	Description
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose • `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.
secretArn	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains username and password required to connect to your database. The secret must contain a JSON structure with the following keys: `{ "username": " database username", "password": " password" }`
version	The version of the template that is currently supported.

How Amazon Q Business connector crawls Amazon RDS (Oracle) ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect a database data source to Amazon Q, Amazon Q crawls user and group information from a column in the source table. You specify this column in the console or using the `configuration` parameter as part of the `CreateDataSource` operation.

If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

A database data source has the following limitations:

- You can only specify an allow list for a database data source. You can't specify a deny list.
- You can only specify groups. You can't specify individual users for the allow list.
- The database column should be a string containing a semicolon delimited list of groups.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Amazon RDS (Oracle) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional

document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q PostgreSQL connector supports the following field mappings:

Supported field mappings

- Document

Document

JDBC field name	Index field name	Description	Data type
jd_document_id	jd_document_id	Custom	String
jd_document_title	jd_document_title	Custom	String
jd_source_uri	_source_uri	Default	String

IAM role for Amazon RDS (Oracle) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
```

```
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Amazon RDS (PostgreSQL) to Amazon Q Business

> **Note**
>
> Amazon RDS (PostgreSQL) connector remains fully supported for existing customers through May 31, 2026. While this connector is no longer available for new users, current users can continue to use it without interruption. We are continuously evolving our connector portfolio to offer more scalable and customizable solutions. For future integrations, we recommend exploring the Amazon Q Business Custom Connector Framework, designed to support a broader range of enterprise use cases with enhanced flexibility.

Amazon RDS (PostgreSQL) is a web service that makes it easier to set up, operate, and scale a relational database in the AWS Cloud. If you are a AWS user, you can use Amazon Q Business to index your Amazon RDS (PostgreSQL) data source.

The Amazon Q Amazon RDS (PostgreSQL) data source connector supports PostgreSQL 9.6.

You can connect your Amazon RDS (PostgreSQL) instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials. Also, avoid adding tables with sensitive data or personal identifiable information (PII).

Topics

- Known limitations for the Amazon RDS (PostgreSQL) connector
- Amazon RDS (PostgreSQL) connector overview
- Prerequisites for connecting Amazon Q Business to Amazon RDS (PostgreSQL)
- Connecting Amazon Q Business to Amazon RDS (PostgreSQL) using the console
- Connecting Amazon Q Business to Amazon RDS (PostgreSQL) using APIs
- How Amazon Q Business connector crawls Amazon RDS (PostgreSQL) ACLs
- Amazon RDS (PostgreSQL) data source connector field mappings
- IAM role for Amazon RDS (PostgreSQL) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Amazon RDS (PostgreSQL) connector

The Amazon RDS (PostgreSQL) connector has the following known limitations:

- Deleted database rows will not be tracked in when Amazon Q checks for updated content.
- The size of field names and values in a row of your database can't exceed 400KB.
- Column names should only contain alphanumeric characters and not spaces.
- If you have a large amount of data in your database data source, and do not want Amazon Q to index all your database content after the first sync, you can choose to sync only new, modified, or deleted documents.

Amazon RDS (PostgreSQL) connector overview

The following table gives an overview of the Amazon RDS (PostgreSQL) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic
	Authentication credentials	• Username of database user • Password of database user
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Driver version	PostgreSQL – 42.3.2
	Data source version	PostgreSQL 9.6
	Identity crawling	No
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Document

Category	Feature	Support
		Note Each database row is considered an individual searchable Amazon Q document. See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Amazon RDS (PostgreSQL)

Before you begin, make sure that you have completed the following prerequisites.

In Amazon RDS (PostgreSQL), make sure you have:

- Noted your database username and password.

> **Important**
>
> As a best practice, provide Amazon Q with read-only database credentials.

- Copied your database host URL, port, and instance. You can find this information on the Amazon RDS console.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.

- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Amazon RDS (PostgreSQL) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Amazon RDS (PostgreSQL) using the console

The following procedure outlines how to connect Amazon Q Business to Amazon RDS (PostgreSQL) using the AWS Management Console.

Connecting Amazon Q to Amazon RDS (PostgreSQL)

1. **Name and description**, do the following:
   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
2. In **Source**, enter the following information:
   a. **Host** – Enter the database host URL, for example: `http://instance URL.region.rds.amazonaws.com`.
   b. **Port** – Enter the database port, for example, `5432`.

c. **Instance** – Enter the database instance, for example `postgres` .

d. **SSL certificate location** – Choose to enter the Amazon S3 path to your SSL certificate file.

3. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

4. In **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. For **Database username**, and **Password** – Enter the authentication credential values you copied from your database.

   c. Choose **Save**.

5. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

   a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

   b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

   For more information, see VPC.

6. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

   > **Note**
   >
   > Creating a new service IAM role is recommended.

   For more information, see IAM role.

7. In **Sync scope**, enter the following information:

- **SQL query** – Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
- **Primary key column** – Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
- **Title column** – Provide the name of the column in your database table that you want to designate as the column with document titles.
- **Body column** – Provide the name of the column in your database table that you want to designate as the column with document body text.

  Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

8. **Advanced settings**

   Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

9. In **Additional configuration – *optional*** – Configure the following settings:

   - **Change-detecting columns** – Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns.
   - **Users' IDs column** – Enter the name of the column which contains User IDs to be allowed access to content.
   - **Groups column** – Enter the name of the column that contains groups to be allowed access to content.
   - **Source URLs column** – Enter the name of the column which contains Source URLs to be indexed.
   - **Time stamps column** – Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.

- **Time zones column** – Enter the name of the column which contains time zones for the content to be crawled.
- **Time stamps format** – Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.

10. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New or modified content sync** – Sync only new and modified documents.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

    For more details, see Sync mode.

11. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
12. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
13. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

14. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Amazon RDS (PostgreSQL) using APIs

You use the `CreateDataSource` action to connect a data source to your Amazon Q application.

Then, you use the `configuration` parameter to provide a JSON schema with all other configuration information specific to your data source connector.

Amazon RDS (PostgreSQL) JSON schema

The following is the Amazon RDS (PostgreSQL) JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
```

```
            "type": "string",
            "enum": [
              "mysql",
              "db2",
              "postgresql",
              "oracle",
              "sqlserver"
            ]
          },
          "dbHost": {
            "type": "string"
          },
          "dbPort": {
            "type": "string"
          },
          "dbInstance": {
            "type": "string"
          }
        },
        "required": [
          "dbType",
          "dbHost",
          "dbPort",
          "dbInstance"
        ]
      }
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "document": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string"
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
```

```
        "timestampColumn": {
          "type": "string"
        },
        "timestampFormat": {
          "type": "string"
        },
        "timezone": {
          "type": "string"
        },
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "serverlessAurora": {
          "type": "string",
          "enum": ["true", "false"]
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
```

```
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
connectionConfiguration	Configuration information for the endpoint for the data source.
repositoryEndpointMetadata	Required configuration information for connecting your data source. • dbType—The type of Java database you are using, whether `mysql`, db2, `postgresql` , `oracle`, or `sqlserver` . • dbHost—The database host name. • dbPort—The database port. • dbInstance—The database instance.

Configuration	Description
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings. Specify the type of data source and the secret ARN.
document	A list of objects that map the attributes or field names of your database content to Amazon Q index field names. For more information, see Fiel.
additionalProperties	Additional configuration options for your content in your data source. Use to include or exclude specific content in your database data source.
primaryKey	Provide the primary key for the database table. This identifies the row in the table for which your SQL query is written. The connector uses the primary key column value to identify rows, detect changes, and crawl data.
titleColumn	Provide the name of the column in your database table that you want to designate as the column with document titles.
bodyColumn	Provide the name of the column in your database table that you want to designate as the column with document body text. Your SQL query can include multiple columns in your table concatenated into a single body column with an assigned alias.

Configuration	Description
sqlQuery	Enter SQL query statements like SELECT and JOIN operations. SQL queries must be less than 1000 characters and not contain any semi-colons (;). Amazon Q will crawl all database content that matches your query.
timestampColumn	Enter the name of the column which contains time stamps. Amazon Q uses time stamp information to detect changes in your content and sync only changed content.
timestampFormat	Enter the name of the column which contains time stamp formats to use to detect content changes and re-sync your content.
timezone	Enter the name of the column which contains time zones for the content to be crawled.
changeDetectingColumns	Enter the names of the columns that Amazon Q will use to detect content changes. Amazon Q will re-index content when there is a change in any of these columns
allowedUsersColumns	Enter the name of the column which contains User IDs to be allowed access to content.
allowedGroupsColumn	Enter the name of the column which contains User IDs to be allowed access to content.
sourceURIColumn	Enter the name of the column which contains Source URLs to be indexed.
isSslEnabled	`true` to add a path to an SSL certificate file stored in an Amazon S3 bucket.
type	The type of data source. Specify `JDBC` as your data source type.

Configuration	Description
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose • `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.
secretArn	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains username and password required to connect to your database. The secret must contain a JSON structure with the following keys: `{ "username": " database username", "password": " password" }`
version	The version of the template that is currently supported.

How Amazon Q Business connector crawls Amazon RDS (PostgreSQL) ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect a database data source to Amazon Q, Amazon Q crawls user and group information from a column in the source table. You specify this column in the console or using the `configuration` parameter as part of the `CreateDataSource` operation.

If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

A database data source has the following limitations:

- You can only specify an allow list for a database data source. You can't specify a deny list.
- You can only specify groups. You can't specify individual users for the allow list.
- The database column should be a string containing a semicolon delimited list of groups.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Amazon RDS (PostgreSQL) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional

document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q PostgreSQL connector supports the following field mappings:

Supported field mappings

- Document

Document

JDBC field name	Index field name	Description	Data type
jd_document_id	jd_document_id	Custom	String
jd_document_title	jd_document_title	Custom	String
jd_source_uri	_source_uri	Default	String

IAM role for Amazon RDS (PostgreSQL) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
```

```
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Amazon Q custom connector to Amazon Q Business

Use a custom data source when you have a repository that Amazon Q Business doesn't yet provide a data source connector for. When you create a custom data source, you have complete control over how the documents to index are selected. Amazon Q only provides metric information that you can use to monitor your data source sync jobs. You must create and run the crawler that determines the documents your data source indexes.

You can use a custom data source connector to:

- See the same run history metrics that Amazon Q data sources provide even when you can't use Amazon Q data sources to sync your repositories.
- Create a consistent sync monitoring experience between Amazon Q data sources and custom data sources.
- See sync metrics for a data source connector that you created using the BatchPutDocument and BatchDeleteDocument API operations.

You can create an Amazon Q custom data source connector using either the AWS Management Console or the CreateDataSource.

When you create a custom data source using the `CreateDataSource` API operation:

- The action returns an ID to use when you synchronize the data source.
- You only need to provide a `Name` and optionally a `Description`.
- Set the `Configuration` parameter as follows:

```
"configuration": {
"type": "CUSTOM",
"version": "1.0.0"
}
```

- When indexing documents later, you must specify the main title of your documents using the Document object, and `_source_uri` in DocumentAttribute. The main title is required so that `DocumentTitle` and `DocumentURI` are included in the ChatSync or Chat response.

When you create a custom data source using the console:

- The console returns an ID to use when you synchronize the data source.
- Give your data source a name, and optionally a description and resource tags.
- After the data source is created, a data source ID is shown. Copy this ID to use when you synchronize the data source with the index.

Topics

- Creating an Amazon Q custom connector
- Required attributes
- Viewing metrics

Creating an Amazon Q custom connector

To use a custom data source, create an application environment that is responsible for updating your Amazon Q index. The application environment depends on a crawler that you create. The crawler reads the documents in your repository and determines which documents should be sent to Amazon Q. Your application environment should perform the following steps:

1. Crawl your repository and make a list of the documents in your repository that are added, updated, or deleted.
2. Call the StartDataSourceSyncJob API operation to signal that a sync job is starting. You provide a data source ID to identify the data source that is synchronizing. Amazon Q returns an execution ID to identify a particular sync job.

   > **Note**
   >
   > After you end a sync job, you can start a new sync job. There can be a period of time before all of the submitted documents are added to the index. To see the status of the sync job, use the ListDataSourceSyncJobs operation. If the `Status` returned for the sync job is `SYNCING_INDEXING`, some documents are still being indexed. You can start a new sync job when the status of the previous job is `FAILED` or `SUCCEEDED`.

3. To remove documents from the index, use the BatchDeleteDocument operation. You provide the data source ID and execution ID to identify the data source that is synchronizing and the job that this update is associated with.
4. To signal the end of the sync job, use the StopDataSourceSyncJob operation. After you call the `StopDataSourceSyncJob` operation, the associated execution ID is no longer valid.

   > **Note**
   >
   > After you call the `StopDataSourceSyncJob` operation, you can't use a sync job identifier in a call to the `BatchPutDocument` or `BatchDeleteDocument` operations. If you do, all of the documents submitted are returned in the `FailedDocuments` response message from the API.

5. To list the sync jobs for the data source and to see metrics for the sync jobs, use the ListDataSourceSyncJobs operation with the index and data source identifiers.

Required attributes

When you submit a document to Amazon Q using the `BatchPutDocument` API operation, you must provide the following two attributes for each document:

- `_data_source_id` – The identifier of the data source. This is returned when you create the data source with either the console or the `CreateDataSource` API operation.

- `_data_source_sync_job_execution_id` – The identifier of the sync run. This is returned when you start the index synchronization with the `StartDataSourceSyncJob` operation.

The following is the JSON required to index a document using a custom data source.

```
{
    "Documents": [
        {
            "Attributes": [
                {
                    "Key": "_data_source_id",
                    "Value": {
                        "StringValue": "data source identifier"
                    }
                },
                {
                    "Key": "_data_source_sync_job_execution_id",
                    "Value": {
                        "StringValue": "sync job identifier"
                    }
                }
            ],
            "Blob": "document content",
            "ContentType": "content type",
            "Id": "document identifier",
            "Title": "document title"
        }
    ],
    "IndexId": "index identifier",
    "RoleArn": "IAM role ARN"
}
```

When you remove a document from the index using the `BatchDeleteDocument` API operation, you must specify the following two fields in the `DataSourceSyncJobMetricTarget` parameter:

- `DataSourceId` – The identifier of the data source. This is returned when you create the data source with either the console or the `CreateDataSource` API operation.
- `DataSourceSyncJobId` – The identifier of the sync run. This is returned when you start the index synchronization with the `StartDataSourceSyncJob` operation.

The following is the JSON required to delete a document from the index using the `BatchDeleteDocument` operation.

```
{
    "DataSourceSyncJobMetricTarget": {
        "DataSourceId": "data source identifier",
        "DataSourceSyncJobId": "sync job identifier"
    },
    "DocumentIdList": [
        "document identifier"
    ],
    "IndexId": "index identifier"
}
```

Viewing metrics

After a sync job is finished, you can use the `DataSourceSyncJobMetrics` API operation to get the metrics associated with the sync job. Use this API operation to monitor your custom data source syncs.

You can submit the same document multiple times, either as part of the `BatchPutDocument` operation, the `BatchDeleteDocument` operation, or if the document is submitted for both addition and deletion, Regardless of how you submit the document, it is only counted once in the metrics.

- `DocumentsAdded` – The number of documents submitted using the `BatchPutDocument` operation associated with this sync job that are added to the index for the first time. If a document is submitted for addition more than once in a sync, the document is only counted once in the metrics.
- `DocumentsDeleted` – The number of documents submitted using the `BatchDeleteDocument` operation associated with this sync job that are deleted from the index. If a document is submitted for deletion more than once in a sync, the document is only counted once in the metrics.
- `DocumentsFailed` – The number of documents associated with this sync job that failed indexing. These documents were accepted by Amazon Q for indexing but could not be indexed or deleted. If a document isn't accepted by Amazon Q, the identifier for the document is returned in the `FailedDocuments` response property of the `BatchPutDocument` and `BatchDeleteDocument` operations.

- `DocumentsModified` – The number of modified documents submitted using the `BatchPutDocument` operation associated with this sync job that were modified in the Amazon Q index.

Amazon Q also emits Amazon CloudWatch metrics while indexing documents. For more information, see Monitoring Amazon Q with Amazon CloudWatch.

Amazon Q doesn't return the `DocumentsScanned` metric for custom data sources.

Connecting Web Crawler to Amazon Q Business

An Amazon Q Business Web Crawler connector crawls and indexes either public facing websites or internal company websites that use HTTPS. With Amazon Q web crawler, you can create a generative AI web experience for your end users based on the website data you crawl using either the AWS Management Console or the `CreateDataSource` API.

> **Note**
>
> Amazon Q Web Crawler supports only HTTPS enabled sites. It doesn't support HTTP or self-signed certificate enabled websites.

> **Important**
>
> When selecting websites to index, you must adhere to the Amazon Acceptable Use Policy and all other Amazon terms. Remember that you must only use Amazon Q Web Crawler to index your own webpages, or webpages that you have authorization to index. To learn how to stop Amazon Q Web Crawler from indexing your websites, see Configuring a `robots.txt` file for Amazon Q Business Web Crawler.

If you receive an error when crawling a website, it could be that the website is blocked from crawling. To crawl internal websites, you can set up a web proxy. The web proxy must be public facing. You can also use authentication to access and crawl websites.

Note

Amazon Q Web Crawler connector does *not* support AWS KMS encrypted Amazon S3 buckets. It supports only server-side encryption with Amazon S3 managed keys.

Topics

- Web Crawler connector overview
- Prerequisites for connecting Amazon Q Business to Web Crawler
- Retrieving XPaths (XML Path Language) for Web Crawler
- Connecting Amazon Q Business to Web Crawler using the console
- Connecting Amazon Q Business to Web Crawler using APIs
- Connecting Amazon Q Business to Web Crawler using AWS CloudFormation
- Web Crawler data source connector field mappings
- IAM role for Amazon Q Business Web Crawler connector
- Configuring a robots.txt file for Amazon Q Business Web Crawler

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Web Crawler connector overview

The following table gives an overview of the Amazon Q Business Web Crawler connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	• Basic • NTLM/Kerberos • Form • SAML **Note** You don't need authentication to crawl public websites you have permission to crawl.
	Authentication credentials	**Basic authentication** • Website username • Website password **NTLM/Kerberos authentication** • NTLM/Kerberos username • NTLM/Kerberos password **Form authentication** • Login page URL • Website username • Website password • Username field Xpath • Password field Xpath • Password button Xpath • (Optional) Username button Xpath

Category	Feature	Support
		SAML authentication • Login page URL • Website username • Website password • Username field Xpath • Password field Xpath • Password button Xpath • (Optional) Username button Xpath
	Access Control List (ACL) crawling	No
	Identity crawling	No
Crawl features	**Custom metadata**	Yes
	Visual content processing	Yes. Amazon Q Business can extract and index content from images embedded in webpages and the following supported document types: PDF, PowerPoint, Microsoft Word (DOCX), Google Slides, Google Docs
	Entities	Yes. The following entities are supported: • Web page • Attachment See What is a document? for more details on what each connector crawls as a document.

Category	Feature	Support
	Field mappings	Yes. For more information, see Field mappings.
	Filters	Yes. The following filters are supported : • Sync specific domains and subdomains • Include files linked on web pages • Regex patterns to crawl and index specific URLs • Regex patterns to crawl and index specific files • Include web pages by crawl depth • Specify maximum file size and links per page for Amazon Q to crawl
	Sync mode	Supports full and new, modified, or deleted content sync
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Web Crawler

Before you begin, make sure that you have completed the following prerequisites.

> **Note**
>
> For more information on connecting Web Crawler to Amazon Q Business, see Index website contents using the Amazon Q Web Crawler connector for Amazon Q Business in the *AWS Machine Learning Blog*.

For Amazon Q Web Crawler, make sure you have:

- Copied the seed or sitemap URLs of the websites that you want to index and stored them in a text file or an Amazon S3 bucket. Each URL must be included on a separate line.
- **For XML sitemaps:** Copied the sitemap XML and saved it in an XML file in an Amazon S3 bucket. You can also combine multiple sitemap XML files into a .zip file.
- **For websites that require basic, NTLM, or Kerberos authentication:**
  - Noted your website authentication credentials, which include a username and password.

    > **Note**
    >
    > Amazon Q Web Crawler supports the NTLM authentication protocol that includes password hashing, and Kerberos authentication protocol that includes password encryption.

- **For websites that require SAML or login form authentication:**
  - Noted your website authentication credentials, which include a username and password.
  - Copied the XPaths (XML Path Language) of the username field (and the username button if using SAML), password field and button, and copied the login page URL. You can find the XPaths of elements using your web browser's developer tools. XPaths follow this format: `//tagname[@Attribute='Value']`.

    > **Note**
    >
    > Amazon Q Web Crawler uses a headless Chrome browser and the information from the form to authenticate and authorize access with an OAuth 2.0 protected URL.

- **Optional:** Copied the host name and the port number of the web proxy server if you want to use a web proxy to connect to internal websites that you want to crawl. The web proxy must be public facing. Amazon Q supports connecting to web proxy servers backed by basic authentication, or you can connect with no authentication.
- **Optional:** Copied the virtual private cloud (VPC) subnet ID if you want to use a VPC to connect to internal websites you want to crawl. For more information, see Using Amazon VPC.

In your AWS account, make sure you have:

- Created an IAM role for your data source and, if using the API, noted the ARN of the IAM role.

- **For websites that require authentication credentials to crawl:** Stored your Web Crawler authentication credentials in an AWS Secrets Manager secret and, if using the API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application environment on the console.

Retrieving XPaths (XML Path Language) for Web Crawler

If the website you are crawling with Amazon Q Business Web Crawler uses Form or SAML authentication, you need to provide Amazon Q with the absolute XPaths for the username and password fields on your web page. Optionally, you may also need to provide the absolute XPaths to the username and password buttons.

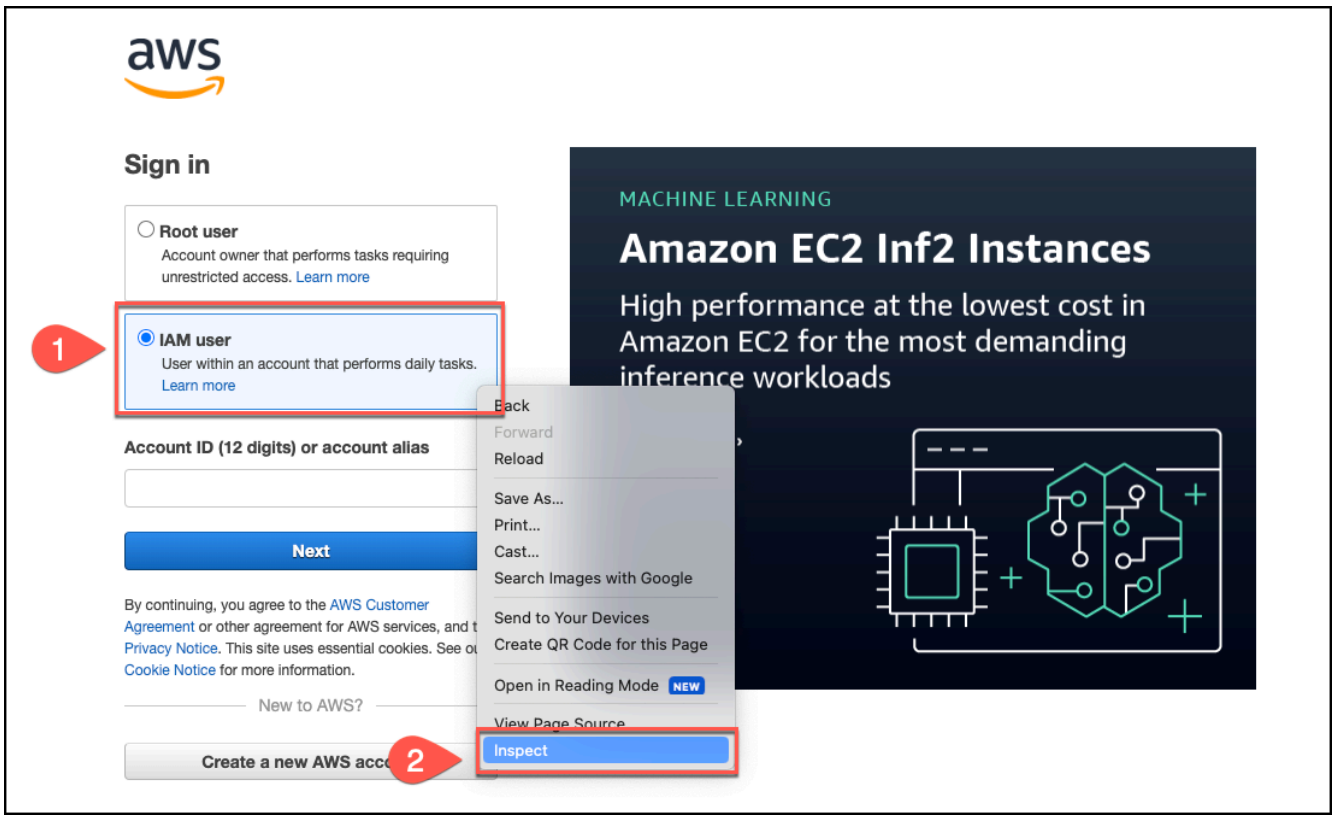
XPaths are expressions used to uniquely identify and locate the content of any XML like language document (including HTML). Amazon Q uses the XPaths you provide to confirm access to the website you want to crawl. XPaths usually follow the following format: `//tagname[@Attribute='Value']`.

The following tabs provide a procedure for retrieving XPaths required for your Amazon Q Web Crawler connector using different web browsers.

Chrome

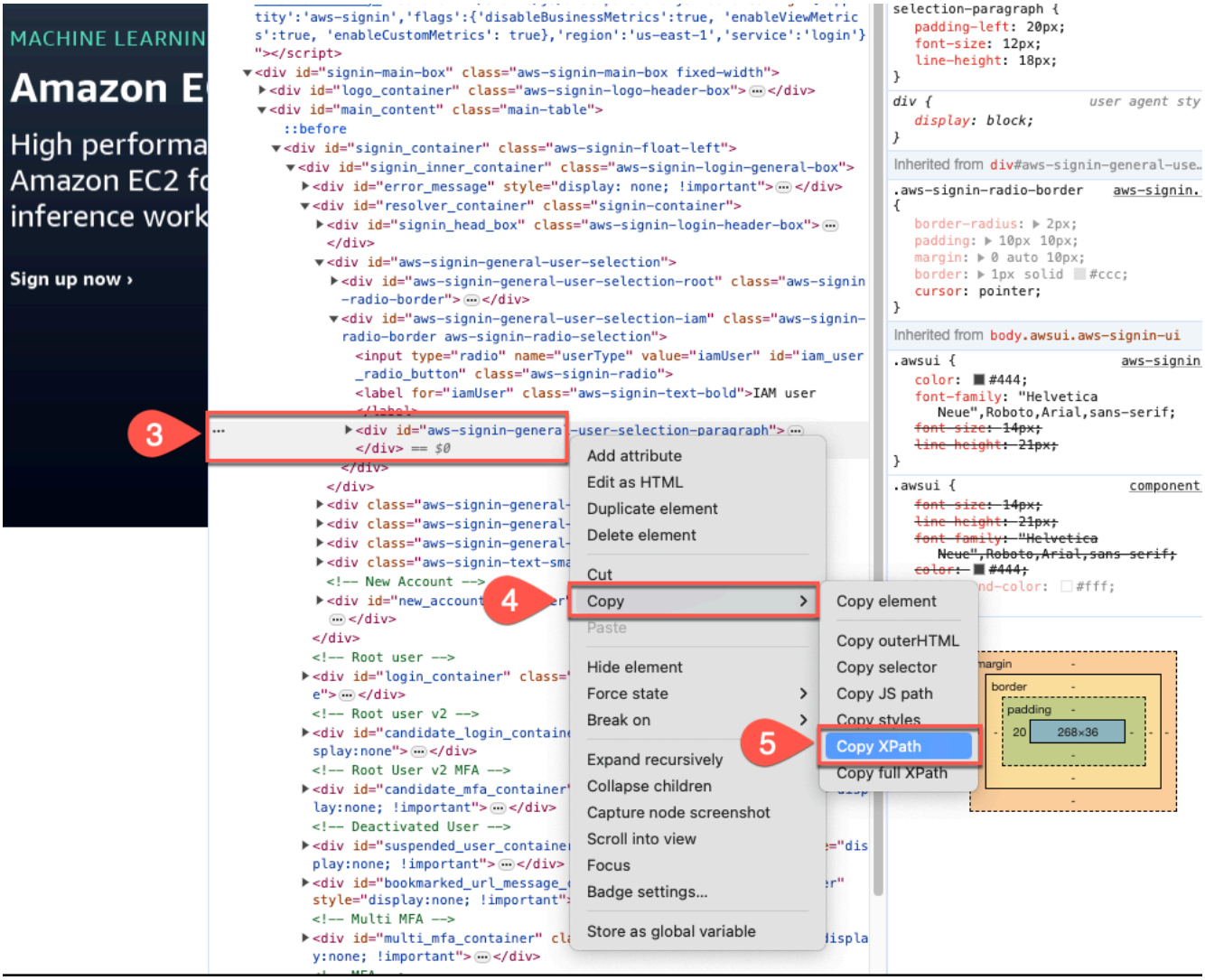
To retrieve XPaths for an Amazon Q Web Crawler

1. Make sure you're on the web page you want to crawl. Then, either select or click on the web page element you want to retrieve the XPath for. This could be the username or password fields, or the username and password buttons.
2. Then, open the context (right-click) menu and then choose the **Inspect** option.



In the **Developer Tools** window that opens, the details for the element you've chosen will be highlighted.

3. Right click on the highlighted element to open the context (right-click) menu.
4. Choose **Copy**.
5. Then, choose **Copy XPath**.



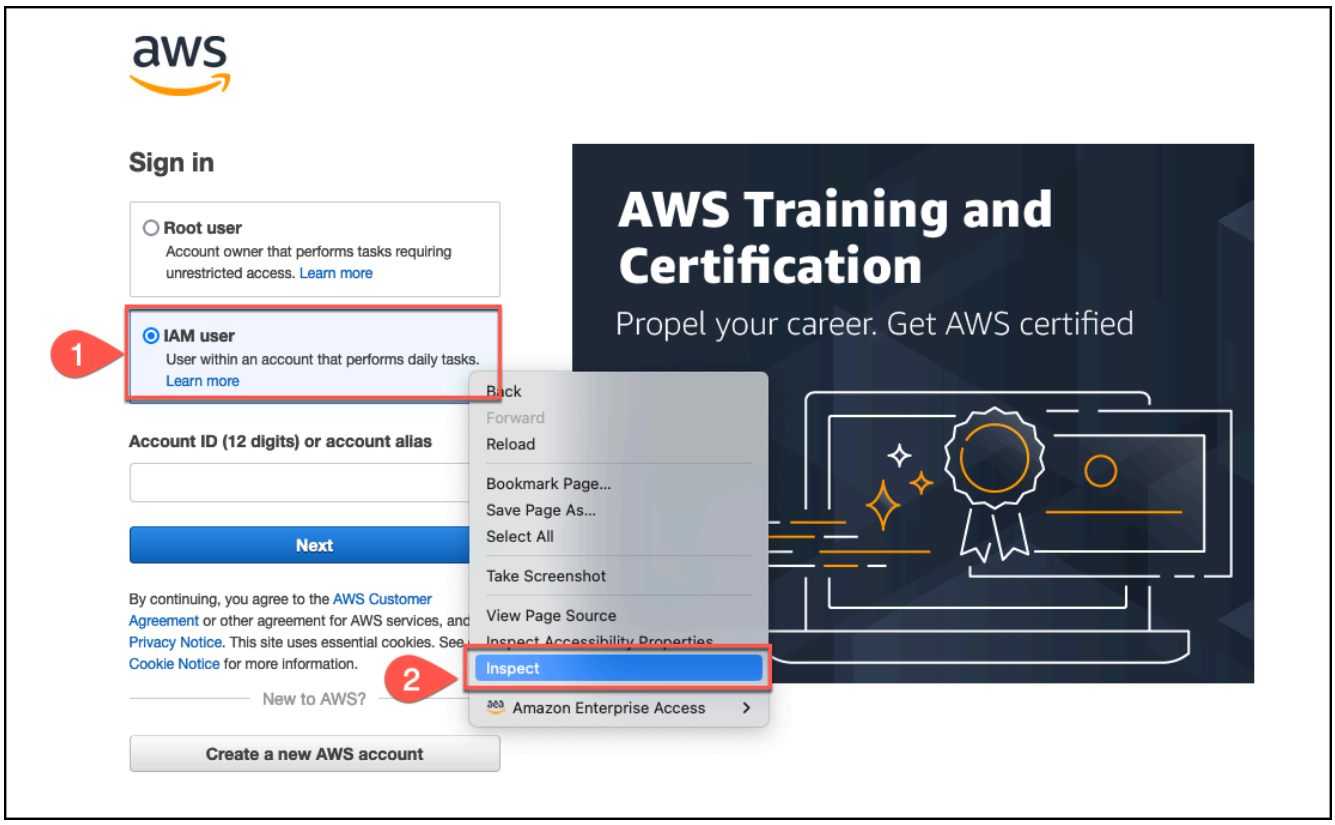
6. Then, open a text editor of your choice and paste the XPath you copied. The format of the XPath will look like this: `//tagname[@Attribute='Value']`.

   Input the relevant XPaths you've copied in the **Authentication** section when you configure Amazon Q Web Crawler connector.

Firefox

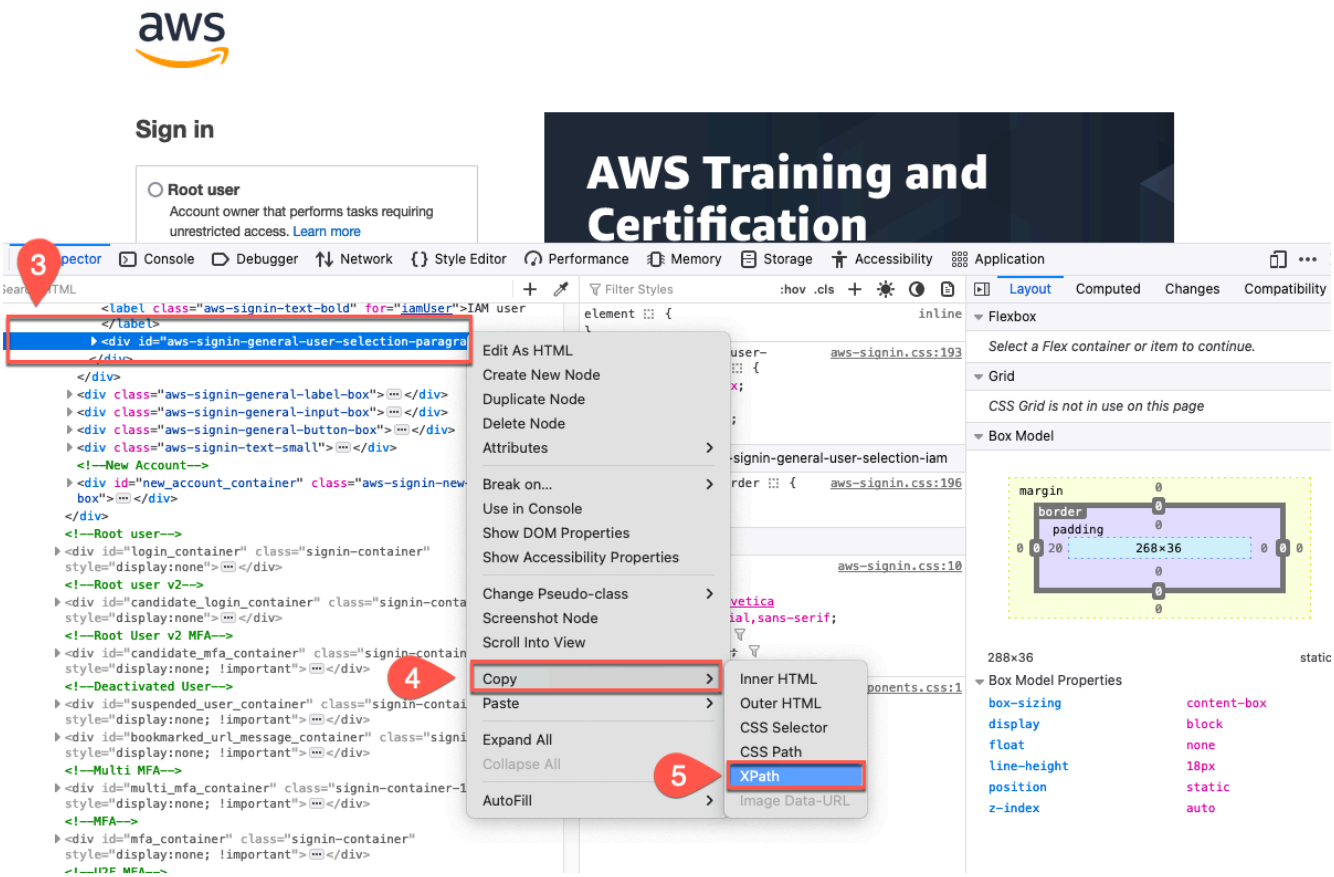
To retrieve XPaths for an Amazon Q Web Crawler

1. Make sure you're on the web page you want to crawl. Then, either select or click on the web page element you want to retrieve the XPath for. This could be the username or password fields, or the username and password buttons.
2. Then, open the context (right-click) menu and then choose the **Inspect** option.



In the **Developer Tools** window that opens, the details for the element you've chosen will be highlighted.

3. Right click on the highlighted element to open the context (right-click) menu.
4. Choose **Copy**.
5. Then, choose **Copy XPath**.



6. Then, open a text editor of your choice and paste the XPath you copied. The format of the XPath will look like this: `//tagname[@Attribute='Value']`.

   Input the relevant XPaths you've copied in the **Authentication** section when you configure Amazon Q Web Crawler connector.

Connecting Amazon Q Business to Web Crawler using the console

The following procedure outlines how to connect Amazon Q Business to Web Crawler using the AWS Management Console.

> **Note**
>
> Before you begin adding your data source, make sure you've created an Amazon Q Business application, and added an index and retriever to it.

Connecting Amazon Q to Web Crawler

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Web Crawler** data source to your Amazon Q application.
5. Then, on the **Web Crawler** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source** choose from the following options:

   - **Source URLs** – Add up to 10 seed/starting point URLs of the websites you want to crawl. You can also include website subdomains.
   - **Source sitemaps** – Add up to 3 sitemap URLs of the websites you want to crawl.
   - **Source URLs file** – Add up to 100 seed/starting point URLs listed in a text file in Amazon S3. Each URL should be on a separate line in the text file.
   - **Source sitemaps file** – Add up to 3 sitemap XML files stored in Amazon S3. You can also zip the XML files.

   > **Note**
   >
   > If you choose to use a text file that includes a list of up to 100 seed URLs or to use a sitemap XML file, you specify the path to the Amazon S3 bucket where your file is stored.

You can also combine multiple sitemap XML files into a .zip file. Otherwise, you can manually enter up to 10 seed or starting point URLs, and up to three sitemap URLs.

Note

If you want to crawl a sitemap, check that the base or root URL is the same as the URLs listed on your sitemap page. For example, if your sitemap URL is *https://example.com/sitemap-page.html*, the URLs listed on this sitemap page should also use the base URL "https://example.com/".

Note

If you want to later edit your data source to change your seed URLs with authentication to sitemaps, you must create a new data source.
Amazon Q configures the data source using the seed URLs endpoint information in the Secrets Manager secret for authentication. Therefore, Amazon Q can't reconfigure the data source when changing to sitemaps.

8. In **Authentication**, choose the type of authentication you want to use and enter the following information in your AWS Secrets Manager secret:

- **No authentication** – Choose to crawl a public website without any authentication.
- **Basic authentication** – Enter a name for the secret, and the username and password you use to access the website you want to crawl.
- **NTLM/Kerberos authentication** – Enter a name for the secret, and the username and password you use to access the website you want to crawl. NTLM authentication protocol includes password hashing, and Kerberos authentication protocol includes password encryption.
- **Form authentication** – Enter a name for the secret, and the username and password you use to access the website you want to crawl. Also add the following values:
  - **User name field Xpath** – Enter the XPath for your user name field. For example, `//input[@id='username']`.
  - **Password field Xpath** – Enter the XPath for your password field. For example, `//input[@id='password']`.

- **User name button Xpath – *Optional*** – Provide the XPath for the button associated with the username input field, typically found on a login page. For example, `//button[@id='login-submit']`. This XPath helps the automation script identify and interact with the button to proceed with the login process. You can find this XPath using your browser's developer tools.
- **Password button Xpath** – Provide the XPath for the button associated with the password input field, typically used to submit the login form. For example, `//button[@id='login-submit']`. This XPath is essential for automating the interaction with the button after the password has been entered. You can find this XPath using your browser's developer tools.

> **Note**
>
> You can find the XPaths (XML Path Language) of elements using your web browser's developer tools. XPaths usually follow this format: `//tagname[@Attribute='Value']`. To learn how to retrieve XPaths, see Retrieving XPaths (XML Path Language) for Web Crawler.

- **SAML authentication** – Enter a name for the secret, and the username and password you use to access the website you want to crawl. Also add the following values:
  - **User name field Xpath** – Enter the XPath for your user name field. For example, `//input[@id='username']`.
  - **Password field Xpath** – Enter the XPath for your password field. For example, `//input[@id='password']`.
  - **User name button Xpath – *Optional*** – Provide the XPath for the button associated with the username input field, typically found on a login page. For example, `//button[@id='login-submit']`. This XPath helps the automation script identify and interact with the button to proceed with the login process. You can find this XPath using your browser's developer tools.
  - **Password button Xpath** – Provide the XPath for the button associated with the password input field, typically used to submit the login form. For example, `//button[@id='login-submit']`. This XPath is essential for automating the interaction with the button after the password has been entered. You can find this XPath using your browser's developer tools.

> **Note**
>
> You can find the XPaths (XML Path Language) of elements using your web browser's developer tools. XPaths usually follow this format: `//tagname[@Attribute='Value']`. To learn how to retrieve XPaths, see Retrieving XPaths (XML Path Language) for Web Crawler.

9. **Web proxy – *optional*** – Enter the host name and the port number of the proxy server that you want to use to connect to internal websites. For example, the host name of *https://a.example.com/page1.html* is "a.example.com" and the port number is 443, the standard port for HTTPS. If web proxy credentials are required to connect to a website host, you can create an AWS Secrets Manager secret that stores the following credentials: the username and password required for the web proxy to log into the host URL.
10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.
11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.
12. In **Sync scope**, enter the following information:

a. **Sync domain range** – Choose whether to sync website domains with subdomains only, or also crawl other domains that the webpages link to (**Sync everything**). By default, Amazon Q only syncs the domains of the websites that you want to crawl.

b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

c. In **Additional configuration – *optional*** – Configure the following settings:

- **Scope settings**, choose from the following:
  - **Crawl depth** – The depth, or number, of levels from the seed level to crawl. For example, the seed URL page is depth 0 and any hyperlinks on this page that are also crawled are depth 1.
  - **Maximum links per page** – The maximum number of URLs on a single webpage to crawl.
  - **Maximum throttling** – The maximum number of URLs crawled per website host per minute.
- **Include files that web pages link to** – Select this option to allow Amazon Q Business to crawl and index files that are linked from webpages.
- **Crawl URL patterns** – Add regular expression patterns to specify which URLs should be included or excluded during the crawling process. This allows you to control which pages on a website are crawled and which hyperlinks on those pages are indexed.
- **URL pattern to index** – Add regular expression patterns to define which URLs or files should be included or excluded from indexing. This helps you focus the indexing process on specific URLs or files, ensuring that only the desired content is indexed.

d. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

To extract audio transcriptions and video content, enable processing for the following file types:

e. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete

phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

13. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

14. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.

15. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.

16. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

    For more information, see Field mappings.

17. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Web Crawler using APIs

To connect Amazon Q Business to Web Crawler using the Amazon Q API, call `CreateDataSource`. Use this API to:

- provide a name and tags for your data source
- an Amazon Resource Name (ARN) of an IAM role with permission to access the data source and required resources
- a sync schedule for Amazon Q to check the documents in your data source
- a Amazon VPC configuration

For more information on available parameters, see CreateDataSource in the Amazon Q API reference.

Provide the seed or starting point URLs, or the sitemap URLs, as part of the connection configuration or repository endpoint details. Also specify the website authentication credentials and authentication type if your websites require authentication, and other necessary configurations.

Topics

- Web Crawler configuration properties
- Web Crawler JSON schema
- Web Crawler JSON schema example

Web Crawler configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`type`	The type of data source.	`string` The only allowed values are • `WEBCRAWLERV2`	Yes
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	`string` You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has the sub-property `repositoryEndpointMetadata`.	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source. This is a sub-property for the `connectionConfiguration`.	`object` This property has the following sub-properties • `authentication` • `seedUrlConnections` • `s3SeedUrl` • `siteMapUrls` • `s3SiteMapUrl`	Yes
`authentication`	The authentication type if your websites require the same authentication. This is a sub-property for the `repositoryEndpointMetadata`.	`string` Depending on your connection type, the allowed values are `NoAuthentication`, `BasicAuth`, `NTLM_Kerberos`, `Form`, SAML.	Yes

Configuration	Description	Type	Required
`seedUrlConnections`	The list of seed or starting point URLs for the websites that you want to crawl. You can list up to 100 seed URLs. This is a sub-property for the `repositoryEndpointMetadata` .	`array` This is an array of `seedUrls`. Use the pattern: [`https://.*`].	No
`seedUrl`	The seed or starting point URL for the websites that you want to crawl. This is a sub-property for the `seedUrlConnections` .	`string` Use the pattern: [`https://.*`].	Yes
`s3SeedUrl`	The S3 path to the text file that stores the list of seed or starting point URLs. This is a sub-property for the `repositoryEndpointMetadata` .	`string` Use the pattern *`s3://bucket-name/directory/`* . Each URL in the text file must be formatted on a separate line. You can list up to 100 seed URLs in a file.	No

Configuration	Description	Type	Required
`siteMapUrls`	The list of sitemap URLs for the websites that you want to crawl. This is a sub-property for the `repositoryEndpointMetadata` .	`array` This is an array of `siteMapUrls` . You can list up to three sitemap URLs. Use the pattern: [`https://.*`].	No
`s3SiteMapUrl`	The S3 path to the sitemap XML files. This is a sub-property for the `repositoryEndpointMetadata` .	`string` Use the pattern, *s3://bucket-name/directory/*. You can list up to three sitemap XML files. You can club together multiple sitemap files into a .zip file and store the .zip file in your Amazon S3 bucket.	No
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties • `webPage` • `attachment`	Yes

Configuration	Description	Type	Required
• webPage • attachments	A list of objects that map the attributes or field names of your webpages and attachments to Amazon Q index field names.	object These properties has the following sub-properties • indexFieldName • indexFieldType • dataSourceFieldName • dateFieldFormat	No
indexFieldName	The name of the index field. This is a sub-property for webPage and attachments .	string	Yes
indexFieldType	The type of the index field. This is a sub-property for webPage and attachments .	string The only allowed value are • STRING • DATE • LONG	Yes
dataSourceFieldName	The field name of the data source. This is a sub-property for webPage and attachments .	string	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The field date of the data source. This is a sub-property for `webPage` and `attachments` .	`string` Use the pattern `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties that are not required • rateLimit • metadataFilesPrefix . • maxFileSize • maxFileSizeInMegaBytes • crawlDepth • maxLinksPerUrl • honorRobots • crawlSubDomain • crawlAllDomain • crawlAttachments • maxFileSizeInMegaBytes • inclusionURLCrawlPatterns	Yes

Configuration	Description	Type	Required
		• exclusionURLCrawlPatterns • inclusionURLIndexPatterns • exclusionURLIndexPatterns • inclusionFileIndexPatterns • exclusionFileIndexPatterns • proxy	
rateLimit	The maximum number of URLs crawled per website host per minute. This is a sub-property of additionalProperties .	string The default value is 300	Yes
maxFileSize	The maximum size (in MB) of a webpage or attachment to crawl. This is a sub-property of additionalProperties .	string The default value is 50	Yes

Configuration	Description	Type	Required
`crawlDepth`	The number of levels from the seed URL to crawl. This is a sub-property of `additionalProperties` .	`string` The seed URL page is depth 1 and any hyperlinks on this page that are also crawled are depth 2. The default value is 2.	Yes
`maxLinksPerUrl`	The maximum number of URLs on a webpage to include when crawling a website. This number is per webpage. As a website's webpages are crawled, any URLs that the webpages link to also are crawled. URLs on a webpage are crawled in order of appearance. This is a sub-property of `additionalProperties` .	`string` The default value is `100`.	Yes

Configuration	Description	Type	Required
honorRobots	true to respect the robots.txt directives of the websites that you want to crawl. These directives control how Amazon Q Web Crawler crawls the websites, and whether Amazon Q can crawl only specific content or not crawl any content. This is a sub-property of additionalProperties . **Note** The honorRobots feature is currently only available if you use the API.	boolean	Yes

Configuration	Description	Type	Required
`crawlSubDomain`	`true` to crawl the website domains with subdomains only. This is a sub-property of `additionalProperties` .	`boolean` If the seed URL is "abc.example.com", then "a.abc.example.com" and "b.abc.example.com" are also crawled. If you don't set `crawlSubDomain` or `crawlAllDomain` to `true`, then Amazon Q only crawls the domains of the websites that you want to crawl.	Yes
`crawlAllDomain`	Crawl the website domains with subdomains and other domains the web pages link to. This is a sub-property of `additionalProperties` .	`boolean` If you don't set `crawlSubDomain` or `crawlAllDomain` to `true`, then Amazon Q only crawls the domains of the websites that you want to crawl.	Yes
`crawlAttachments`	`true` to crawl files that the webpages link to. This is a sub-property of `additionalProperties` .	`boolean`	Yes

Configuration	Description	Type	Required
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. This is a sub-property of `additionalProperties` .	`string` The default value is `50`. The maximum file size should be greater than `0` and less than or equal to `50`.	No

Configuration	Description	Type	Required
• `inclusionURLCrawlPatterns` • `inclusionURLIndexPatterns`	These are sub-properties of `additionalProperties` . A list of regular expression patterns to *include* crawling certain URLs and indexing any hyperlinks on these URL webpages. URLs that match the patterns are included in the index. URLs that don't match the patterns are excluded from the index. If a URL matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the URL and website's webpages aren't included in the index.	`array(string)`	No

Configuration	Description	Type	Required
• `exclusionURLCrawlPatterns` • `exclusionURLIndexPatterns`	These are sub-properties of `additionalProperties` . A list of regular expression patterns to *exclude* crawling certain URLs and indexing any hyperlinks on these URL webpages. URLs that match the patterns are excluded from the index. URLs that don't match the patterns are included in the index. If a URL matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the URL/website's webpages aren't included in the index.	`array(string)`	No

Configuration	Description	Type	Required
`inclusionFileIndexPatterns`	This is a sub-property of `additionalProperties` . A list of regular expression patterns to *include* certain web page files. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.	`array(string)`	No

Configuration	Description	Type	Required
`exclusionFileIndexPatterns`	This is a sub-property of `additionalProperties` . A list of regular expression patterns to *exclude* certain webpage files. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.	`array(string)`	No
`proxy`	This is a sub-property of `additionalProperties` . Configuration information required to connect to your internal websites through a web proxy.	`object`	No

Configuration	Description	Type	Required
`host`	This is a sub-property of `proxy`. The host name of the proxy server that you want to use to connect to internal websites. For example, the host name of *https://a.example.com/page1.html* is a `.example.com .`	`string`	No
`port`	This is a sub-property of `proxy`. The port number of the proxy server that you want to use to connect to internal websites. For example, the port 443 would be `443`.	`string`	No

Configuration	Description	Type	Required

`secretArn`	This is a sub-property of `proxy`. If web proxy credentials are required to connect to a website host, you can create an AWS Secrets Manager secret that stores the credentials. Provide the Amazon Resource Name (ARN) of the secret.	`string`
		
		The minimum length is 20and the maximum length is 2,048 characters
		
		The JSON structure for this is
		
		`{ "userName": string, "password": string }`
			No

Configuration	Description	Type	Required
secretArn	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that's used if your websites require authentication to access the websites. You store the authentication credentials for the website in the secret that contains JSON key-value pairs. If you use basic, or NTLM/Kerberos, enter the username and password. The JSON keys in the secret must be userName and password. NTLM authentication protocol includes password hashing, and Kerberos authentication protocol includes password encryption. If you use SAML or form authentication, enter the username and password, XPath for the username	If you use seedUrlConnections or s3SeedUrl as the connection type, you can choose from all authentication values (NoAuthentication , BasicAuth , NTLM_Kerberos , Form, SAML) depending on the use case. If you use siteMapUrls or s3SiteMapUrl as connection type, the authentication should be NoAuthentication . You must use the following JSON structure for your authentication values. • For BasicAuth /NTLM_Kerberos {	No

Configuration	Description	Type	Required

	field (and username button if using SAML), XPaths for the password field and button, and the login page URL. The JSON keys in the secret must be `userName`, `password`, `userNameFieldXpath`, `userNameButtonXpath`, `passwordFieldXpath`, `passwordButtonXpath`, and `loginPageUrl`. You can find the XPaths (XML Path Language) of elements using your web browser's developer tools. XPaths usually follow this format: `//tagname[@Attribute='Value']`.
	
	Amazon Q also checks if the endpoint information (seed URLs) included in the secret is the
		<pre>{
		"userName": String,
		"password": String
		}</pre>
		• For Form/SAML
		<pre>{
		"loginPageUrl": String,
		"userName": String,
		"password": String,
		"userNameFieldXpath": String,
		"passwordFieldXpath": String,
		"userNameButtonXpath": String,
		"passwordButtonXpath": String
		}</pre>	

Configuration	Description	Type	Required
	same the endpoint information specified in your data source endpoint configuration details.	**Note** XML Path Language (XPaths) of elements can be found using the web browser's developer tools. XPaths usually follow this format: `//tagname[@Attribute='Value']`.	
`version`	The version of this template that's currently supported.	`string` The default value is `1.0.0`.	No
`implicitWaitDuration`	Specifies how long the connector will wait, in seconds, before crawling a webpage.	Range: 0-10 eg. "implicitWaitDuration": "5"	

Web Crawler JSON schema

The following is the Web Crawler JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["WEBCRAWLERV2", "WEBCRAWLER"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FORCED_FULL_CRAWL", "FULL_CRAWL"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "siteMapUrls": {
              "type": "array",
              "items": {
                "type": "string",
                "pattern": "https://.*"
              }
            },
            "s3SeedUrl": {
              "type": ["string", "null"],
              "pattern": "s3:.*"
            },
            "s3SiteMapUrl": {
              "type": ["string", "null"],
              "pattern": "s3:.*"
            },
            "seedUrlConnections": {
              "type": "array",
              "items": [
```

```
                {
                  "type": "object",
                  "properties": {
                    "seedUrl": {
                      "type": "string",
                      "pattern": "https://.*"
                    }
                  },
                  "required": ["seedUrl"]
                }
              ]
            },
            "authentication": {
              "type": "string",
              "enum": [
                "NoAuthentication",
                "BasicAuth",
                "NTLM_Kerberos",
                "Form",
                "SAML"
              ]
            }
          }
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "webPage": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
```

```
                    "enum": ["STRING", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "attachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
```

```
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "rateLimit": {
        "type": "string",
        "default": "300"
      },
      "maxFileSize": {
        "type": "string",
        "default": "50"
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "crawlDepth": {
        "type": "string",
        "default": "2"
      },
      "maxLinksPerUrl": {
        "type": "string",
        "default": "100"
      },
      "crawlSubDomain": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
```

```
            }
          ],
          "default": false
        },
        "crawlAllDomain": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "honorRobots": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "crawlAttachments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "inclusionURLCrawlPatterns": {
          "type": "array",
          "items": {
            "type": "string"
```

```
          }
        },
        "exclusionURLCrawlPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionURLIndexPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionURLIndexPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileIndexPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileIndexPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "proxy": {
          "type": "object",
          "properties": {
            "host": {
              "type": "string"
            },
            "port": {
              "type": "string"
            },
            "secretArn": {
              "type": "string",
              "minLength": 20,
```

```
              "maxLength": 2048
            }
          }
        },
        "implicitWaitDuration":  {
          "type":"object",
          "properties": {
            "innerNumber" : {
              "type": "number",
              "minimum": 0,
              "maximum": 10
            }
          }
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": [
        "rateLimit",
        "maxFileSize",
        "crawlDepth",
        "crawlSubDomain",
        "crawlAllDomain",
        "maxLinksPerUrl",
        "honorRobots"
      ]
    }
  },
  "version": {
    "type": "string",
```

```
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "type",
    "syncMode",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

Web Crawler JSON schema example

The following is the Web Crawler JSON schema example:

```
{
  "type": "WEBCRAWLERV2",
  "syncMode": "FULL_CRAWL",
  "secretArn": "arn:aws:secretsmanager:us-west-2:0123456789012:secret",
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "siteMapUrls": ["https://example.com/sitemap.xml"],
      "s3SeedUrl": "s3://bucket/seed-url",
      "s3SiteMapUrl": "s3://bucket/sitemap-url",
      "seedUrlConnections": [
        {
          "seedUrl": "https://example.com"
        }
      ],
      "authentication": "NoAuthentication"
    }
  },
  "repositoryConfigurations": {
    "webPage": {
      "fieldMappings": [
        {
          "indexFieldName": "title",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "page_title",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
```

```
        }
      ]
    },
    "attachment": {
      "fieldMappings": [
        {
          "indexFieldName": "attachment_title",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "attachment_name",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    }
  },
  "additionalProperties": {
    "rateLimit": "300",
    "maxFileSize": "50",
    "crawlDepth": "2",
    "maxLinksPerUrl": "100",
    "crawlSubDomain": "true",
    "crawlAllDomain": "true",
    "honorRobots": "true"
  }
}
```

Connecting Amazon Q Business to Web Crawler using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- Web Crawler configuration properties
- Web Crawler JSON schema for using the configuration property with AWS CloudFormation
- Web Crawler YAML schema for using the configuration property with AWS CloudFormation

Web Crawler configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`type`	The type of data source.	`string` The only allowed values are • `WEBCRAWLERV2`	Yes
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	`string` You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required
connectionConfiguration	Configuration information for the endpoint for the data source.	object This property has the sub-property repositoryEndpointMetadata .	Yes
repositoryEndpointMetadata	The endpoint information for the data source. This is a sub-property for the connectionConfiguration .	object This property has the following sub-properties • authentication • seedUrlConnections • s3SeedUrl • siteMapUrls • s3SiteMapUrl	Yes
authentication	The authentication type if your websites require the same authentication. This is a sub-property for the repositoryEndpointMetadata .	string Depending on your connection type, the allowed values are NoAuthentication , BasicAuth , NTLM_Kerberos , Form, SAML.	Yes

Configuration	Description	Type	Required
`seedUrlConnections`	The list of seed or starting point URLs for the websites that you want to crawl. You can list up to 100 seed URLs. This is a sub-property for the `repositoryEndpointMetadata` .	`array` This is an array of `seedUrls`. Use the pattern: [`https://.*`].	No
`seedUrl`	The seed or starting point URL for the websites that you want to crawl. This is a sub-property for the `seedUrlConnections` .	`string` Use the pattern: [`https://.*`].	Yes
`s3SeedUrl`	The S3 path to the text file that stores the list of seed or starting point URLs. This is a sub-property for the `repositoryEndpointMetadata` .	`string` Use the pattern *`s3://bucket-name/directory/`* . Each URL in the text file must be formatted on a separate line. You can list up to 100 seed URLs in a file.	No

Configuration	Description	Type	Required
`siteMapUrls`	The list of sitemap URLs for the websites that you want to crawl. This is a sub-property for the `repositoryEndpointMetadata` .	`array` This is an array of `siteMapUrls` . You can list up to three sitemap URLs. Use the pattern: [`https://.*`].	No
`s3SiteMapUrl`	The S3 path to the sitemap XML files. This is a sub-property for the `repositoryEndpointMetadata` .	`string` Use the pattern, *s3://bucket-name/directory/*. You can list up to three sitemap XML files. You can club together multiple sitemap files into a .zip file and store the .zip file in your Amazon S3 bucket.	No
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties • `webPage` • `attachment`	Yes

Configuration	Description	Type	Required
• webPage • attachments	A list of objects that map the attributes or field names of your webpages and attachments to Amazon Q index field names.	object These properties has the following sub-properties • indexFieldName • indexFieldType • dataSourceFieldName • dateFieldFormat	No
indexFieldName	The name of the index field. This is a sub-property for webPage and attachments .	string	Yes
indexFieldType	The type of the index field. This is a sub-property for webPage and attachments .	string The only allowed value are • STRING • DATE • LONG	Yes
dataSourceFieldName	The field name of the data source. This is a sub-property for webPage and attachments .	string	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The field date of the data source. This is a sub-property for `webPage` and `attachments` .	`string` Use the pattern `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties that are not required • rateLimit • metadataFilesPrefix . • maxFileSize • maxFileSizeInMegaBytes • crawlDepth • maxLinksPerUrl • honorRobots • crawlSubDomain • crawlAllDomain • crawlAttachments • maxFileSizeInMegaBytes • inclusionURLCrawlPatterns	Yes

Configuration	Description	Type	Required
		• `exclusionURLCrawlPatterns` • `inclusionURLIndexPatterns` • `exclusionURLIndexPatterns` • `inclusionFileIndexPatterns` • `exclusionFileIndexPatterns` • `proxy`	
`rateLimit`	The maximum number of URLs crawled per website host per minute. This is a sub-property of `additionalProperties` .	`string` The default value is `300`	Yes
`maxFileSize`	The maximum size (in MB) of a webpage or attachment to crawl. This is a sub-property of `additionalProperties` .	`string` The default value is `50`	Yes

Configuration	Description	Type	Required
`crawlDepth`	The number of levels from the seed URL to crawl. This is a sub-property of `additionalProperties` .	`string` The seed URL page is depth 1 and any hyperlinks on this page that are also crawled are depth 2. The default value is 2.	Yes
`maxLinksPerUrl`	The maximum number of URLs on a webpage to include when crawling a website. This number is per webpage. As a website's webpages are crawled, any URLs that the webpages link to also are crawled. URLs on a webpage are crawled in order of appearance. This is a sub-property of `additionalProperties` .	`string` The default value is `100`.	Yes

Configuration	Description	Type	Required
honorRobots	true to respect the robots.txt directives of the websites that you want to crawl. These directives control how Amazon Q Web Crawler crawls the websites, and whether Amazon Q can crawl only specific content or not crawl any content. This is a sub-property of additionalProperties . **Note** The honorRobots feature is currently only available if you use the API.	boolean	Yes

Configuration	Description	Type	Required
`crawlSubDomain`	`true` to crawl the website domains with subdomains only. This is a sub-property of `additionalProperties` .	`boolean` If the seed URL is "abc.example.com", then "a.abc.example.com" and "b.abc.example.com" are also crawled. If you don't set `crawlSubDomain` or `crawlAllDomain` to `true`, then Amazon Q only crawls the domains of the websites that you want to crawl.	Yes
`crawlAllDomain`	Crawl the website domains with subdomains and other domains the web pages link to. This is a sub-property of `additionalProperties` .	`boolean` If you don't set `crawlSubDomain` or `crawlAllDomain` to `true`, then Amazon Q only crawls the domains of the websites that you want to crawl.	Yes
`crawlAttachments`	`true` to crawl files that the webpages link to. This is a sub-property of `additionalProperties` .	`boolean`	Yes

Configuration	Description	Type	Required
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. This is a sub-property of `additionalProperties` .	`string` The default value is `50`. The maximum file size should be greater than `0` and less than or equal to `50`.	No

Configuration	Description	Type	Required
• `inclusionURLCrawlPatterns` • `inclusionURLIndexPatterns`	These are sub-properties of `additionalProperties` . A list of regular expression patterns to *include* crawling certain URLs and indexing any hyperlinks on these URL webpages. URLs that match the patterns are included in the index. URLs that don't match the patterns are excluded from the index. If a URL matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the URL and website's webpages aren't included in the index.	`array(string)`	No

Configuration	Description	Type	Required
• `exclusionURLCrawlPatterns` • `exclusionURLIndexPatterns`	These are sub-properties of `additionalProperties` . A list of regular expression patterns to *exclude* crawling certain URLs and indexing any hyperlinks on these URL webpages. URLs that match the patterns are excluded from the index. URLs that don't match the patterns are included in the index. If a URL matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the URL/website's webpages aren't included in the index.	`array(string)`	No

Configuration	Description	Type	Required
`inclusionFileIndexPatterns`	This is a sub-property of `additionalProperties` . A list of regular expression patterns to *include* certain web page files. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.	`array(string)`	No

Configuration	Description	Type	Required
`exclusionFileIndexPatterns`	This is a sub-property of `additionalProperties` . A list of regular expression patterns to *exclude* certain webpage files. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.	`array(string)`	No
`proxy`	This is a sub-property of `additionalProperties` . Configuration information required to connect to your internal websites through a web proxy.	`object`	No

Configuration	Description	Type	Required
`host`	This is a sub-property of `proxy`. The host name of the proxy server that you want to use to connect to internal websites. For example, the host name of *https://a.example.com/page1.html* is a `.example.com .`	`string`	No
`port`	This is a sub-property of `proxy`. The port number of the proxy server that you want to use to connect to internal websites. For example, the port 443 would be `443`.	`string`	No

Configuration	Description	Type	Required

`secretArn`	This is a sub-property of `proxy`. If web proxy credentials are required to connect to a website host, you can create an AWS Secrets Manager secret that stores the credentials. Provide the Amazon Resource Name (ARN) of the secret.	`string`
		
		The minimum length is 20and the maximum length is 2,048 characters
		
		The JSON structure for this is
		
		`{ "userName": string, "password": string }`
			No

Configuration	Description	Type	Required
`secretArn`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that's used if your websites require authentication to access the websites. You store the authentication credentials for the website in the secret that contains JSON key-value pairs. If you use basic, or NTLM/Kerberos, enter the username and password. The JSON keys in the secret must be `userName` and `password`. NTLM authentication protocol includes password hashing, and Kerberos authentication protocol includes password encryption. If you use SAML or form authentication, enter the username and password, XPath for the username	If you use `seedUrlConnections` or `s3SeedUrl` as the connection type, you can choose from all authentication values (`NoAuthentication`, `BasicAuth`, `NTLM_Kerberos`, `Form`, SAML) depending on the use case. If you use `siteMapUrls` or `s3SiteMapUrl` as connection type, the `authentication` should be `NoAuthentication`. You must use the following JSON structure for your `authentication` values. • For `BasicAuth` /`NTLM_Kerberos` `{`	No

Configuration	Description	Type	Required

	field (and username button if using SAML), XPaths for the password field and button, and the login page URL. The JSON keys in the secret must be `userName`, `password`, `userNameFieldXpath`, `userNameButtonXpath`, `passwordFieldXpath`, `passwordButtonXpath`, and `loginPageUrl`. You can find the XPaths (XML Path Language) of elements using your web browser's developer tools. XPaths usually follow this format: `//tagname[@Attribute='Value']`.
	
	Amazon Q also checks if the endpoint information (seed URLs) included in the secret is the
		<pre>{
		"userName": String,
		"password": String
		}</pre>
		• For Form/SAML
		<pre>{
		"loginPageUrl": String,
		"userName": String,
		"password": String,
		"userNameFieldXpath": String,
		"passwordFieldXpath": String,
		"userNameButtonXpath": String,
		"passwordButtonXpath": String
		}</pre>	

Configuration	Description	Type	Required
	same the endpoint information specified in your data source endpoint configuration details.	**Note** XML Path Language (XPaths) of elements can be found using the web browser's developer tools. XPaths usually follow this format: `//tagname[@Attribute='Value']`.	
`version`	The version of this template that's currently supported.	`string` The default value is `1.0.0`.	No
`implicitWaitDuration`	Specifies how long the connector will wait, in seconds, before crawling a webpage.	Range: 0-10 eg. "implicitWaitDuration": "5"	

Web Crawler JSON schema for using the configuration property with AWS CloudFormation

The following is the Web Crawler JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- Web Crawler JSON schema for using the configuration property with AWS CloudFormation
- Web Crawler JSON schema example for using the configuration property with AWS CloudFormation

Web Crawler JSON schema for using the configuration property with AWS CloudFormation

The following is the Web Crawler JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["WEBCRAWLERV2"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FORCED_FULL_CRAWL", "FULL_CRAWL"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "siteMapUrls": {
              "type": "array",
              "items": {
                "type": "string",
                "pattern": "https://.*"
              }
```

```
            },
            "s3SeedUrl": {
              "type": ["string", "null"],
              "pattern": "s3:.*"
            },
            "s3SiteMapUrl": {
              "type": ["string", "null"],
              "pattern": "s3:.*"
            },
            "seedUrlConnections": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "seedUrl": {
                      "type": "string",
                      "pattern": "https://.*"
                    }
                  },
                  "required": ["seedUrl"]
                }
              ]
            },
            "authentication": {
              "type": "string",
              "enum": [
                "NoAuthentication",
                "BasicAuth",
                "NTLM_Kerberos",
                "Form",
                "SAML"
              ]
            }
          }
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "webPage": {
          "type": "object",
```

```
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "attachment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
```

```
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "rateLimit": {
        "type": "string",
        "default": "300"
      },
      "maxFileSize": {
        "type": "string",
        "default": "50"
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "crawlDepth": {
        "type": "string",
        "default": "2"
      },
```

```
        "maxLinksPerUrl": {
          "type": "string",
          "default": "100"
        },
        "crawlSubDomain": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "crawlAllDomain": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "honorRobots": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "crawlAttachments": {
          "anyOf": [
            {
              "type": "boolean"
```

```
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "inclusionURLCrawlPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionURLCrawlPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionURLIndexPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionURLIndexPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileIndexPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileIndexPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
```

```
        "proxy": {
          "type": "object",
          "properties": {
            "host": {
              "type": "string"
            },
            "port": {
              "type": "string"
            },
            "secretArn": {
              "type": "string",
              "minLength": 20,
              "maxLength": 2048
            }
          }
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": [
        "rateLimit",
        "maxFileSize",
        "crawlDepth",
        "crawlSubDomain",
        "crawlAllDomain",
        "maxLinksPerUrl",
        "honorRobots"
      ]
    }
  },
```

```
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "type",
    "syncMode",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

Web Crawler JSON schema example for using the configuration property with AWS CloudFormation

The following is the Web Crawler JSON schema example for the configuration property for CloudFormation

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation Web Crawler Data Source Template",
  "Resources": {
    "DataSourceWebCrawler": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MyWebCrawlerDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "WEBCRAWLERV2",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:0123456789012:secret",
          "connectionConfiguration": {
            "repositoryEndpointMetadata": {
              "siteMapUrls": ["https://example.com/sitemap.xml"],
              "s3SeedUrl": "s3://bucket/seed-url",
              "s3SiteMapUrl": "s3://bucket/sitemap-url",
```

```
            "seedUrlConnections": [
              {
                "seedUrl": "https://example.com"
              }
            ],
            "authentication": "BasicAuth"
          }
        },
        "repositoryConfigurations": {
          "webPage": {
            "fieldMappings": [
              {
                "indexFieldName": "title",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "page_title",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          },
          "attachment": {
            "fieldMappings": [
              {
                "indexFieldName": "attachment_title",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "attachment_name",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          }
        },
        "additionalProperties": {
          "rateLimit": "300",
          "maxFileSize": "50",
          "crawlDepth": "2",
          "maxLinksPerUrl": "100",
          "crawlSubDomain": "true",
          "crawlAllDomain": "true",
          "honorRobots": "true"
        }
      }
    }
  }
}
```

```
}
```

Web Crawler YAML schema for using the configuration property with AWS CloudFormation

The following is the Web Crawler YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- Web Crawler YAML schema for using the configuration property with AWS CloudFormation
- Web Crawler YAML schema example for using the configuration property with AWS CloudFormation

Web Crawler YAML schema for using the configuration property with AWS CloudFormation

The following is the Web Crawler YAML schema for the configuration property for CloudFormation.

```
type: object
properties:
  type:
    type: string
    enum:
      - WEBCRAWLERV2
  syncMode:
    type: string
    enum:
      - FORCED_FULL_CRAWL
      - FULL_CRAWL
  secretArn:
    type: string
    minLength: 20
    maxLength: 2048
  connectionConfiguration:
    type: object
    properties:
      repositoryEndpointMetadata:
        type: object
        properties:
          siteMapUrls:
            type: array
            items:
              type: string
              pattern: https://.*
```

```
          s3SeedUrl:
            type:
              - string
              - null
            pattern: s3:.*
          s3SiteMapUrl:
            type:
              - string
              - null
            pattern: s3:.*
          seedUrlConnections:
            type: array
            items:
              type: object
              properties:
                seedUrl:
                  type: string
                  pattern: https://.*
              required:
                - seedUrl
          authentication:
            type: string
            enum:
              - NoAuthentication
              - BasicAuth
              - NTLM_Kerberos
              - Form
              - SAML
    required:
      - repositoryEndpointMetadata
  repositoryConfigurations:
    type: object
    properties:
      webPage:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
```

```
                type: string
                enum:
                  - STRING
                  - DATE
                  - LONG
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: yyyy-MM-dd'T'HH:mm:ss'Z'
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    attachment:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - DATE
                  - LONG
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: yyyy-MM-dd'T'HH:mm:ss'Z'
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
  additionalProperties:
```

```
    type: object
    properties:
      rateLimit:
        type: string
        default: "300"
      maxFileSize:
        type: string
        default: "50"
      maxFileSizeInMegaBytes:
        type: string
      crawlDepth:
        type: string
        default: "2"
      maxLinksPerUrl:
        type: string
        default: "100"
      crawlSubDomain:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
        default: false
      crawlAllDomain:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
        default: false
      honorRobots:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
        default: false
      crawlAttachments:
        anyOf:
          - type: boolean
          - type: string
```

```
        enum:
          - "true"
          - "false"
    default: false
  inclusionURLCrawlPatterns:
    type: array
    items:
      type: string
  exclusionURLCrawlPatterns:
    type: array
    items:
      type: string
  inclusionURLIndexPatterns:
    type: array
    items:
      type: string
  exclusionURLIndexPatterns:
    type: array
    items:
      type: string
  inclusionFileIndexPatterns:
    type: array
    items:
      type: string
  exclusionFileIndexPatterns:
    type: array
    items:
      type: string
  proxy:
    type: object
    properties:
      host:
        type: string
      port:
        type: string
      secretArn:
        type: string
        minLength: 20
        maxLength: 2048
  enableDeletionProtection:
    anyOf:
      - type: boolean
      - type: string
        enum:
```

```
              - "true"
              - "false"
        default: false
      deletionProtectionThreshold:
        type: string
        default: "15"
    required:
      - rateLimit
      - maxFileSize
      - crawlDepth
      - crawlSubDomain
      - crawlAllDomain
      - maxLinksPerUrl
      - honorRobots
version:
  type: string
  anyOf:
    - pattern: 1.0.0
required:
  - type
  - syncMode
  - connectionConfiguration
  - repositoryConfigurations
  - additionalProperties
```

Web Crawler YAML schema example for using the configuration property with AWS CloudFormation

The following is the Web Crawler YAML example for the Configuration property for CloudFormation:

```
AWSTemplateFormatVersion: 2010-09-09
Description: CloudFormation Web Crawler Data Source Template
Resources:
  DataSourceWebCrawler:
    Type: AWS::QBusiness::DataSource
    Properties:
      ApplicationId: app12345-1234-1234-1234-123456789012
      IndexId: indx1234-1234-1234-1234-123456789012
      DisplayName: MyWebCrawlerDataSource
      RoleArn: arn:aws:iam::123456789012:role/qbusiness-data-source-role
      Configuration:
        type: WEBCRAWLERV2
```

```
        syncMode: FULL_CRAWL
        secretArn: arn:aws:secretsmanager:us-west-2:0123456789012:my-webcrawler-secret
        connectionConfiguration:
          repositoryEndpointMetadata:
            siteMapUrls:
              - https://example.com/sitemap.xml
            s3SeedUrl: s3://bucket/seed-url
            s3SiteMapUrl: s3://bucket/sitemap-url
            seedUrlConnections:
              - seedUrl: https://example.com
            authentication: BasicAuth
        repositoryConfigurations:
          webPage:
            fieldMappings:
              - indexFieldName: title
                indexFieldType: STRING
                dataSourceFieldName: page_title
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
          attachment:
            fieldMappings:
              - indexFieldName: attachment_title
                indexFieldType: STRING
                dataSourceFieldName: attachment_name
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
        additionalProperties:
          rateLimit: "300"
          maxFileSize: "50"
          crawlDepth: "2"
          maxLinksPerUrl: "100"
          crawlSubDomain: "true"
          crawlAllDomain: "true"
          honorRobots: "true"
```

Web Crawler data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.

- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Web Crawler connector supports the following entities and the associated reserved and custom attributes.

Supported entities and field mappings

- Web Pages
- Attachments

Web Pages

Web Crawler field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
title	_document_title	Default	String
htmlSize	wc_html_size	Custom	Long (numeric)

Attachments

Web Crawler field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
fileName	wc_file_name	Custom	String
fileType	wc_file_type	Custom	String
fileSize	wc_file_size	Custom	Long (numeric)

IAM role for Amazon Q Business Web Crawler connector

To connect Web Crawler to Amazon Q Business, you must give Amazon Q an IAM role that has the following permissions.

If you're crawling a public website with no authentication:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store operations to ingest access control information from documents.

```
{
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
```

```
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        }
```

If you're crawling a website which uses authentication:

- Permission to access the AWS Secrets Manager secret that contains the credentials to connect to websites or a web proxy server backed by basic authentication.

```
{
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        }
```

If your Secrets Manager secret is decrypted, add permissions for a AWS KMS key to decrypt the username and password secret stored by Secrets Manager:

```
{
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
```

```
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        }
```

If your Amazon Q data source connector needs access to an object stored in an Amazon S3 bucket—like seed URLs or sitemaps— you must add the following permissions to your IAM role:

> **Note**
>
> Check that the file path to the object in your Amazon S3 bucket is of the following format: *s3://BucketName/FolderName/FileName.extension*.

```
{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        }
```

If you are using an Amazon VPC, you need to add the following VPC access permissions to your policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:111122223333:subnet/[[subnet_ids]]",
                "arn:aws:ec2:us-east-1:111122223333:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_111122223333_application-id_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_111122223333_application-id_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAmazonQServicePrincipal",
            "Effect": "Allow",
            "Principal": {
                "Service": "qbusiness.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnEquals": {
                    "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
                }
            }
        }
    ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Configuring a `robots.txt` file for Amazon Q Business Web Crawler

The `robots.txt` file is a standard used to implement the Robots Exclusion Protocol, allowing website owners to specify which parts of their site visiting web crawlers and robots can access. Amazon Q Business Web Crawler adheres to the rules set in your website's `robots.txt` file, which determines the areas it is allowed or not allowed to visit. Amazon Q Business Web Crawler respects standard robots.txt directives like `Allow` and `Disallow`. To control how Amazon Q Business Web Crawler interacts with your website, you can simply adjust these rules in your robots.txt file.

Topics

- Configuring how Amazon Q Web Crawler accesses your website
- Stopping Amazon Q Web Crawler from crawling your website

Configuring how Amazon Q Web Crawler accesses your website

You can control how the Amazon Q Web Crawler indexes your website using `Allow` and `Disallow` directives. You can also control which web pages are indexed and which web pages are not crawled.

To allow Amazon Q Web Crawler to crawl all web pages except disallowed web pages, use the following directive:

```
User-agent: amazon-QBusiness    # Amazon Q Web Crawler
Disallow: /credential-pages/ # disallow access to specific pages
```

To allow Amazon Q Web Crawler to crawl only specific web pages, use the following directive:

```
User-agent: amazon-QBusiness   # Amazon Q Web Crawler
Allow: /pages/ # allow access to specific pages
```

To allow Amazon Q Web Crawler to crawl all website content and disallow crawling for any other robots, use the following directive:

```
User-agent: amazon-QBusiness # Amazon Q Web Crawler
Allow: / # allow access to all pages
User-agent: * # any (other) robot
Disallow: / # disallow access to any pages
```

Stopping Amazon Q Web Crawler from crawling your website

You can stop Amazon Q Web Crawler from indexing your website using the `Disallow` directive. You can also control which web pages are crawled and which aren't.

To stop Amazon Q Web Crawler from crawling the website, use the following directive:

```
User-agent: amazon-QBusiness # Amazon Q Web Crawler
Disallow: / # disallow access to any pages
```

If you have any questions or concerns about Amazon Q Web Crawler, you can reach out to the AWS support team.

Connecting Asana to Amazon Q Business (Preview)

> **Note**
>
> The Asana connector is in preview release and is subject to change.

Asana is a tool for organizing and assigning tasks among users. You can connect a Asana instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the Amazon Q Business Asana connector (Preview)
- Asana connector overview (Preview)
- Prerequisites for connecting Amazon Q Business to Asana (Preview)
- Connecting Amazon Q Business to Asana using the console (Preview)
- Connecting Amazon Q Business to Asana using APIs (Preview)
- Amazon Q Business Asana data source connector field mappings (Preview)
- IAM role for Amazon Q Business Asana connector (Preview)
- Understand error codes in the Amazon Q Business Asana connector (Preview)

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Amazon Q Business Asana connector (Preview)

The Asana connector has the following known limitations:

- Asana supports crawling on only Public Projects.

Asana connector overview (Preview)

The following table gives an overview of the Amazon Q Business Asana connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Service Account and PAT
Authentication credentials	• Service Account Tokens • Personal Access Token	
Access Control List (ACL) crawling	No. For preview, this connector only scans public Asana projects. For more information, see ACL crawling.	
Identity crawling	No	
VPC	Yes	
Crawl features	**Custom metadata**	No
Entities	Yes. The following entities are supported: • Project • Tasks • Comments	

Category	Feature	Support
	Note Each instance of an entity is crawled as a single document.	
Field mappings	Yes. For more information, see Field mappings.	
Filters	Yes. The following filters are supported: • Specific Projects • Project inclusion regex pattern • Project exclusion regex pattern	
Sync mode	Supports full and incremental sync.	
Crawled as a document	• Project • Task • Comment	

Prerequisites for connecting Amazon Q Business to Asana (Preview)

Before you begin, make sure that you have completed the following prerequisites.

In Asana, make sure you have:

- Generated an access token.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Asana authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Asana using the console (Preview)

The following procedure outlines how to connect Amazon Q Business to Asana using the AWS Management Console.

Connecting Amazon Q to Asana

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **asana** data source to your Amazon Q application.
5. Then, on the **Asana** data source page, enter the following information:
6. **Name and description**, do the following:

    - For **Data source name** – Name your data source for easy tracking.

    > **Note**
    >
    > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. In **Sync scope, Workspace ID** – Enter your workspace Id.
8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
9. **Authentication** – Enter your service account token or personal access token.
10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.
11. **Identity crawler** – Amazon Q crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.
12. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.
13. **Sync scope** –

    - In Select workspace – Select content to sync using a specific Workspace ID.
    - Select Project – Select content to sync using All or Specific Project IDs.

- All comments – Select to include all comments.

14. **Additional configuration – optional** – Configure the following settings:

    - In Additional configuration – select from the following options
    - Project regex patterns – Choose to include or exclude specific project names using regex patterns.
    - Document deletion safeguard - optional–To safeguard your documents from deletion during a sync job, select On and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

15. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.

16. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.

17. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

    For more information, see Field mappings.

18. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Asana using APIs (Preview)

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

JSON schema

The following is the Asana JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
```

```
            "authType": {
              "type": "string",
              "enum": [
                "PAT",
                "ServiceAccount"
              ]
            }
          },
          "required": [
            "authType"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "project": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": [
                        "STRING",
                        "DATE",
                        "STRING_LIST",
                        "LONG"
                      ]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
```

```
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      }
    },
    "task": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": [
                    "STRING",
                    "DATE",
                    "STRING_LIST",
                    "LONG"
                  ]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
```

```
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        }
      },
      "comment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "DATE",
                      "STRING_LIST",
                      "LONG"
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
```

```
              }
            ]
          }
        }
      }
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "workspaceIds": {
          "type": "array",
          "items": {
            "type": "string"
          },
          "minItems": 1,
          "maxItems": 1
        },
        "projectIds": {
          "type": "array",
          "items": {
            "type": "string",
            "minLength": 12,
            "maxLength": 16
          },
          "maxItems": 20
        },
        "fieldForUserId": {
          "type": "string"
        },
        "isCrawlAcl": {
          "type": "boolean"
        },
        "isCrawlComments": {
          "type": "boolean"
        },
        "inclusionProjectNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionProjectNamePatterns": {
          "type": "array",
```

```
          "items": {
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "type": "boolean",
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      }
    },
    "enableIdentityCrawler": {
      "type": "boolean"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FULL_CRAWL",
        "FORCED_FULL_CRAWL"
      ]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "type": {
      "type": "string",
      "pattern": "ASANA"
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "connectionConfiguration",
```

```
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the endpoint of the data source.
`repositoryEndpointMetadata`	The endpoint information for the data source.
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.
• `project` • `task` • `comment`	A list of Asana objects and their metadata attributes that Amazon Q crawls and maps to Amazon Q index field names. The Asana data source field names must exist in your Asana custom metadata.
`secretARN`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Asana.
`additionalProperties` • `workspaceIds` • `projectIds`	Additional configuration options for your content in your data source.
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.

Configuration	Description
`inclusionProjectNamePatterns`	A list of regular expression patterns to *include* specific projects in your Asana data source. projects that match the patterns are included in the index. Projects that don't match the patterns are excluded from the index. If a project matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.
`exclusionProjectNamePatterns`	A list of regular expression patterns to *exclude* specific projects in your Asana data source. Projects that match the patterns are excluded from the index. Projects that don't match the patterns are included in the index. If a project matches both an exclusion and inclusion pattern, the exclusion pattern takes precedenc e, and the file isn't included in the index.
`isCrawlComments`	Input `true` to index these types of content.
isCrawlACL	Input must be `False` as Asana does not support document crawling with ACL.
`type`	Specify `ASANA` as your data source type.

Configuration	Description
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.
`enableIdentityCrawler`	This will always be false as Asana does not support Identity Crawling. Identity crawler is activated by default. Crawling identity information on users and groups with access to certain documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.

Configuration	Description
`version`	The version of the template that's currently supported.

Amazon Q Business Asana data source connector field mappings (Preview)

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application environment and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Asana connector supports the following entities and the associated reserved and custom attributes.

Supported entities and field mappings

- Projects
- Tasks
- Comments

Projects

Amazon Q supports crawling Asana Projects and offers the following project field mappings.

Asana field name	Index field name	Description	Data type
projectPermaLink	_source_uri	Default	String
projectCreatedDate	_created_at	Default	Date
projectModifiedDate	_last_updated_at	Default	Date
catagory	_catagory	Default	String
isArchived	asana_archived	Custom	Custom
dueOn	asana_dueOn	Custom	Date
startOn	asana_startOn	Custom	String
isPublicProject	asana_isPublicProject	Custom	String
ownerId	asana_ownerId	Custom	String
ownerName	asana_ownerName	Custom	String
teamId	asana_teamId	Custom	String list
teamName	asana_teamName	Custom	String list
workspaceId	asana_workspaceId	Custom	String
workspaceName	asana_wor kspaceName	Custom	String
isOrganization	asana_isOrganization	Custom	String

Tasks

Amazon Q supports crawling Asana Tasks and offers the following project field mappings.

Asana field name	Index field name	Description	Data type
taskPermaLink	_source_uri	Default	String
taskCreatedDate	_created_at	Default	Date
taskModifiedDate	_last_update_at	Default	Date
category	_category	Default	String
assigneeId	asana_assigneeId	Custom	String
assigneeName	asana_assigneeName	Custom	String
isCompleted	asana_isCompleted	Custom	String
dueOn	asana_dueOn	Custom	String
isSubtask	asana_isSubtask	Custom	String
topLevelTaskId	asana_topLevelTaskId	Custom	String
topLevelTaskName	asana_topLevelTask Name	Custom	String
section Id	asana_sectionId	Custom	String
sectionName	asana_sectionName	Custom	String
projectId	asana_projectId	Custom	String
projectName	asana_projectName	Custom	String
workspaceId	asana_workspaceId	Custom	String
workspaceName	asana_wor kspaceName	Custom	String

Asana field name	Index field name	Description	Data type
isOrganization	asana_isOrganization	Custom	String

Comments

Amazon Q supports crawling Asana Comments and offers the following project field mappings.

Asana field name	Index field name	Description	Data type
commentPermaLink	_source_uri	Default	String
category	_category	Default	String
taskId	asana_taskId	Custom	String
taskName	asana_taskName	Custom	String
teamId	asana_teamId	Custom	String
teamName	asana_teamName	Custom	String
sectionId	asana_sectionId	Custom	String
sectionName	asana_sectionName	Custom	String
projectId	asana_projectId	Custom	String
projectName	asana_projectName	Custom	String
workspaceId	asana_workspaceId	Custom	String
workspaceName	asana_workspaceName	Custom	String
isOrganization	asana_isOrganization	Custom	String

IAM role for Amazon Q Business Asana connector (Preview)

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
```

```
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
```

```
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
```

```
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the Amazon Q Business Asana connector (Preview)

The following table provides information about error codes you may see for the Asana connector and suggested resolutions.

Error code	Error message	Suggested resolution
ASN-5101	The token in your data source configuration is missing.	Enter valid token (specific to PAT or ServiceAccount) and try again.
ASN-5102	The auth type in your data source configuration is invalid.	Enter valid auth type (PAT or ServiceAccount) and try again.
ASN-5103	The auth type in your data source configuration is missing.	Enter valid auth type (PAT or ServiceAccount) and try again.
ASN-5104	The crawl type in your data source configuration is missing.	Enter valid crawlType (ex. FULL_CRAWL) and try again.
ASN-5105	Only String, String List, Date and Long formats are supported for the	Please provide the supported format only for the indexFieldType in all the fieldMappings.

Error code	Error message	Suggested resolution
	indexFieldType in all the field mappings.	
ASN-5106	There was an error parsing the field value. The size has exceeded the maximum allowable limit.	The maximum size permitted is 1000 for the field {field name}. Ex – field name can be token, workspaceId, projectId
ASN-5107	The connection configura tion in your data source configuration is missing.	Enter valid connection configuration details and try again.
ASN-5108	The repository credentia ls in your data source configuration is missing.	Enter valid repository credentials details and try again.
ASN-5109	The repository endpoint metadata in your data source configuration is missing.	Enter valid repository endpoint metadata details and try again.
ASN-5110	The additional propertie s in your data source configuration is missing.E rror message	Enter valid additional properties and try again.
ASN-5111	Invalid Workspace Id.	Provide numeric value for workspace Id.
ASN-5112	Invalid Project Id.	Provide numeric value for Project Id.
ASN-5113	The workspaceIds field has exceeded the limit. Allowed entries are limited to 1.	Correct the number of entries and try again.

Error code	Error message	Suggested resolution
ASN-5114	The projectIds field has exceeded the limit. Maximum allowed entries are 20.	Correct the number of entries and try again.
ASN-5115	The regex pattern provided in {pattern field} Patterns is invalid.	Provide valid regex pattern.
ASN-5116	The workspace Id in your data source configura tion is missing.	Enter a single workspace Id and try again.
ASN-5200	IO Exception occurred while reading contents from Asana.	Rerun the connector once again, if the issue persists contact support.
ASN-5201	Unknown exception occurred.	Rerun the connector once again, if the issue persists contact support.
ASN-5202	The user details are not found.	Verify the user data using the user API curl command or in postman for the given authentication type.
ASN-5204	Could not find Project(s) using the filter provided in the Asana configura tion. Either Workspace (s) or Project(s) access is forbidden.	Check the Workspace and Project(s) access and provide valid inclusion and exclusion project name filter inputs.
ASN-5500	Asana connection successful.	This is to convey the connection to Asana data source is successful.

Connecting Box to Amazon Q Business

Box is a cloud storage service that offers file hosting capabilities. You can connect your Box instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the Box connector
- Box connector overview
- Prerequisites for connecting Amazon Q Business to Box
- Connecting Amazon Q Business to Box using the console
- Connecting Amazon Q Business to Box using APIs
- How Amazon Q Business connector crawls Box ACLs
- Box data source connector field mappings
- IAM role for Box connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Box connector

The Amazon Q Box connector has the following known limitations:

- Crawling data from external folders is not supported.
- When Access Control Lists (ACLs) are enabled, the "Sync only new or modified content" option is not available due to Box API limitations. We recommend using "Full sync" or "New, modified, or deleted content sync" modes instead, or disable ACLs if you need to use this sync mode.

Box connector overview

The following table gives an overview of the Amazon Q Business Box connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Token with JWT Auth by Box
	Authentication credentials	• Client ID • Client secret • Public Key ID • Private Key • Pass Phrase **Important** Admin privileges required.
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Files • Comments • Tasks • Web links

Category	Feature	Support
		See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include web links • Include comments • Include tasks • Include/exclude by file name • Include/exclude by file type • Include/exclude by file path
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Box

Before you begin, make sure that you have completed the following prerequisites.

In Box, make sure you have:

- A Box Enterprise or Box Enterprise Plus account.
- Created a Box custom app in the Box Developer Console and configured it to use **Server Authentication (with JWT)**.
- Set your **App Access Level** to **App + Enterprise Access** and allowed it to **Make API calls using the as-user header**.
- Used the admin user to add the following **Application Scopes** in your Box app:
  - Write all files and folders stored in a Box
  - Manage users
  - Manage groups

  - Manage enterprise properties
- Generated and downloaded Public/Private key pair including a client ID, a client secret, a public key ID, private key ID, a pass phrase, and an enterprise ID to use as authentication credentials. See Public and private keypair for more details.
- Copied your Box enterprise ID either from your Box Developer Console settings or from your Box app. For example, *801234567*.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Box authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

> **Note**
>
> For more information on connecting Box to Amazon Q Business, see Discover insights from Box with the Amazon Q Box connector in the *AWS Machine Learning Blog*.

Connecting Amazon Q Business to Box using the console

The following procedure outlines how to connect Amazon Q Business to Box using the AWS Management Console.

Connecting Amazon Q to Box

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Box** data source to your Amazon Q application.
5. Then, on the **Box** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. **Source** – Enter your **Box enterprise ID**.
8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
9. In **Authentication** – Choose to create an **AWS Secrets Manager secret** and then enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. **Client ID** – The client ID provided by Box.

   c. **Client Secret** – The client secret provided by Box.

   d. **Public Key ID** – Your Box public key ID.

   e. **Private Key** – The private key provided by Box.

   f. **Pass Phrase** – The pass phrase you use to log into your Box account.

10. **Identity crawler** – Amazon Q crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.
11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.
12. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.
13. In **Sync scope**, enter the following information:

    a. **Select additional kinds of content to index** – Choose whether to include **Web links**, **Comments**, and **Tasks**.

    > **Note**
    >
    > Box files are indexed by default.

    b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

    c. **Additional configuration – *optional*** – Configure the following settings:

- **Regex patterns** – Regular expression patterns to include or exclude certain files. You can add up to 100 patterns.

d. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. For **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

- **Full sync** – Sync all content regardless of the previous sync status.
- **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

15. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
16. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
17. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

18. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Box using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Box JSON schema

The following is the Box JSON schema:

```
{
```

```
"$schema": "http://json-schema.org/draft-04/schema#",
"type": "object",
"properties": {
  "connectionConfiguration": {
    "type": "object",
    "properties": {
      "repositoryEndpointMetadata": {
        "type": "object",
        "properties": {
          "enterpriseId": {
            "type": "string",
            "minLength": 1,
            "maxLength": 64
          }
        },
        "required": [
          "enterpriseId"
        ]
      }
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "file": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "STRING_LIST",
```

```
                    "DATE",
                    "LONG"
                  ]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "task": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": [
                    "STRING",
                    "STRING_LIST",
                    "DATE",
                    "LONG"
```

```
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      },
      "comment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "STRING_LIST",
                      "DATE",
                      "LONG"
                    ]
                  },
```

```
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "webLink": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": [
                    "STRING",
                    "STRING_LIST",
                    "DATE",
                    "LONG"
                  ]
                },
                "dataSourceFieldName": {
                  "type": "string"
```

```
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "isCrawlAcl": {
        "type": "boolean"
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "fieldForUserId": {
        "type": "string"
      },
      "crawlComments": {
        "type": "boolean"
      },
      "crawlTasks": {
        "type": "boolean"
      },
      "crawlWebLinks": {
        "type": "boolean"
      },
      "inclusionPatterns": {
        "type": "array",
```

```
          "items": {
            "type": "string"
          }
        },
        "exclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        }
      },
      "required": []
    },
    "type": {
      "type": "string",
      "pattern": "BOX"
    },
    "enableIdentityCrawler": {
      "type": "boolean"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FULL_CRAWL",
        "FORCED_FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "connectionConfiguration",
```

```
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type",
    "enableIdentityCrawler"

  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the endpoint for the data source.
`repositoryEndpointMetadata`	The endpoint information for the data source.
`enterpriseId`	The Box enterprise id.
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.
• `file` • `task` • `comment` • `webLink`	A list of objects that map the attributes or field names of your Box files, tasks, comments, and webLinks to Amazon Q index field names.
`additionalProperties`	Additional configuration options for your content in your data source.
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

Configuration	Description
`isCrawlAcl`	Specify `true` to crawl access control informati on from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.
`crawlComments`	Specify `true` to crawl assets.
`crawlTasks`	Specify `true` to crawl pages.
`crawlWebLinks`	Specify `true` to crawl pages.
• `InclusionPatterns` • `ExclusionPatterns`	A list of regular expression patterns to include or exclude specific content from your Box data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.
`type`	The type of data source. Specify B0X as your data source type.

Configuration	Description
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/principal informati on on users and groups with access to specific documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.

Configuration	Description
secretArn	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Box. The secret must contain a JSON structure with the following keys: `{ "clientID": " client-id ", "clientSecret": " client-secret ", "publicKeyID": " public-key-id ", "privateKey": " private-key ", "passphrase": " pass-phrase " }`
version	The version of this template that's currently supported.

How Amazon Q Business connector crawls Box ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

Roles/permissions: The Box connector translates Box permissions into ACLs that are compatible with Amazon Q Business. There are seven primary roles with permissions:

- Co-owner - Has full control, can change advanced folder settings
- Editor - Has read/write access, can view, download, edit, delete, and manage sharing.
- Viewer - Has read-only access, can preview and download
- Uploader - Has limited write access, can only upload and see names
- Viewer Uploader - A combination of Viewer and Uploader capabilities
- Previewer - Has limited read access, can only preview items
- Previewer Uploader - A combination of Previewer and Uploader capabilities

Permission Inheritance: Files/subfolders inherit permissions from parent folders by default. Permissions follow a "waterfall" design where individuals have access to the folder they are invited into and any subfolders beneath it. Changing permissions on subfolders will result in an error because collaboration is only changeable at the item where it was created.

Identity Crawling: Individual user and group synchronization is supported via email addresses. Each user gets a unique user ID, even if recreated with the same email address. Permissions are tied to user IDs, not email addresses.

Change Management: ACL changes are supported in change log mode, including collaboration invites, accepts, and role changes.

Failure handling: The connector implements a fail-close approach for API failures, with rate limiting handled through queue-based wait time with exponential backoff. Documents are skipped from ingestion rather than being made publicly accessible when permission-related issues occur.

For more information, see Key data source connector concepts.

Box data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

Important

Filtering using document attributes in chat is only supported through the API.

The Amazon Q Box connector supports the following entities and the associated reserved and custom attributes.

Supported entities and field mappings

- Files and folders
- Comments
- Tasks
- Web links

Files and folders

Box field name	Index field name	Description	Data type
bx_createdAt	_created_at	Default	Date
bx_modifiedAt	_last_updated_at	Default	Date
bx_authors	_authors	Default	String list
bx_uri	_source_uri	Default	String
bx_size	bx_file_size	Custom	String
bx_category	_category	Default	String

Comments

Box field name	Index field name	Description	Data type
bx_createdAt	_created_at	Default	Date
bx_modifiedAt	_last_updated_at	Default	Date

Box field name	Index field name	Description	Data type
bx_author	_authors	Custom	String
bx_parentFile	bx_comment_item	Custom	String
bx_category	_category	Default	String

Tasks

Box field name	Index field name	Description	Data type
bx_createdAt	_created_at	Default	Date
bx_action	bx_task_action	Custom	String
bx_taskComplete	bx_task_completed	Custom	String
bx_taskItem	bx_task_item	Custom	String
bx_taskAssigned	bx_task_assigned_to	Custom	String
bx_author	bx_author	Custom	String
bx_category	_category	Default	String
bx_uri	_source_uri	Default	String

Web links

Box field name	Index field name	Description	Data type
bx_createdAt	_created_at	Default	Date
bx_author	bx_author	Custom	String
bx_category	_category	Default	String
bx_uri	_source_uri	Default	String

IAM role for Box connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
```

```
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
```

```
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
```

```
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Confluence (Cloud) to Amazon Q Business

Atlassian Confluence is a collaborative work-management tool designed for sharing, storing, and working on project planning, software development, and product management. You can connect Confluence (Cloud) instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Confluence (Cloud) connector overview
- Prerequisites for connecting Amazon Q Business to Confluence (Cloud)
- Setting up Confluence (Cloud) for connecting to Amazon Q Business
- Connecting Amazon Q Business to Confluence (Cloud) using the console
- Connecting Amazon Q Business to Confluence (Cloud) using APIs
- Connecting Amazon Q Business to Confluence (Cloud) using AWS CloudFormation
- How Amazon Q Business connector crawls Confluence (Cloud) ACLs
- Amazon Q Business Confluence (Cloud) data source connector field mappings
- IAM role for Amazon Q Confluence (Cloud) connector
- Understand error codes in the Amazon Q Business Confluence (Cloud) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.

- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Confluence (Cloud) connector overview

The following table contains an overview of the Amazon Q Business Confluence (Cloud) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic, OAuth 2.0 with Refresh Token Flow
	Authentication credentials	For Basic authentication • Confluence Cloud URL • Confluence username • Password (Confluence (Cloud) site token) For OAuth 2.0 authentication with Refresh Token Flow • App key • App secret • Access token • Refresh token **Note** Access and refresh tokens expire in 1 hour. For information on regenerating tokens, see Atlassian Developer Documentation.

Category	Feature	Support
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Space • Page • Blog post • Comment • Attachment See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Inclusion exclusion filters for **Space key** and **Space URL** • Inclusion exclusion filters on **File Type** for **Attachment entity** • Supports regex filters for entities • Supports inclusion and exclusion filters for **File size**
	Sync mode	Supports full and incremental (new, modified, and deleted) sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Confluence (Cloud)

Before you begin, make sure that you have completed the following prerequisites.

In Confluence Cloud, make sure you have:

- Copied your Confluence instance URL. For example: *`https://example.atlassian.net`*. You need your Confluence instance URL to connect to Amazon Q.
- Configured basic authentication credentials containing a username (email ID used to log into Confluence) and password (Confluence API token) to allow Amazon Q to connect to your Confluence instance. For information about how to create a Confluence API token, see Manage API tokens for your Atlassian account on the Atlassian website.
- **Optional:** Configured OAuth 2.0 credentials containing a Confluence app key, Confluence app secret, Confluence access token, and Confluence refresh token to allow Amazon Q to connect to your Confluence instance. If your access token expires, you can either use the refresh token to regenerate your access token and refresh token pair, or you can repeat the authorization process. For more information about access tokens, see Manage OAuth access tokens on the Atlassian website.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- If you want to have Amazon Q automatically rotate your secret, ensure that your IAM role includes the `secretsmanager:PutSecretValue` and `secretsmanager:UpdateSecret` permissions.
- Stored your Confluence (Cloud) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

> **Note**
>
> For more information on connecting Confluence (Cloud) to Amazon Q Business, see Index your Atlassian Confluence Cloud contents using the Amazon Q Confluence Cloud connector for Amazon Q Business in the *AWS Machine Learning Blog*.

Setting up Confluence (Cloud) for connecting to Amazon Q Business

Before you connect Confluence (Cloud) to Amazon Q Business, you need to create and retrieve the Confluence (Cloud) credentials you will use to connect Confluence (Cloud) to Amazon Q. You will also need to add any permissions needed by Confluence (Cloud) to connect to Amazon Q.

The following sections give you an overview of how to configure Confluence (Cloud) to connect to Amazon Q using either basic authentication or OAuth 2.0 authentication.

Topics

- Basic authentication
- OAuth 2.0 authentication
- How Amazon Q works with Confluence (Cloud) access and refresh tokens
- Checking Confluence (Cloud) connectivity

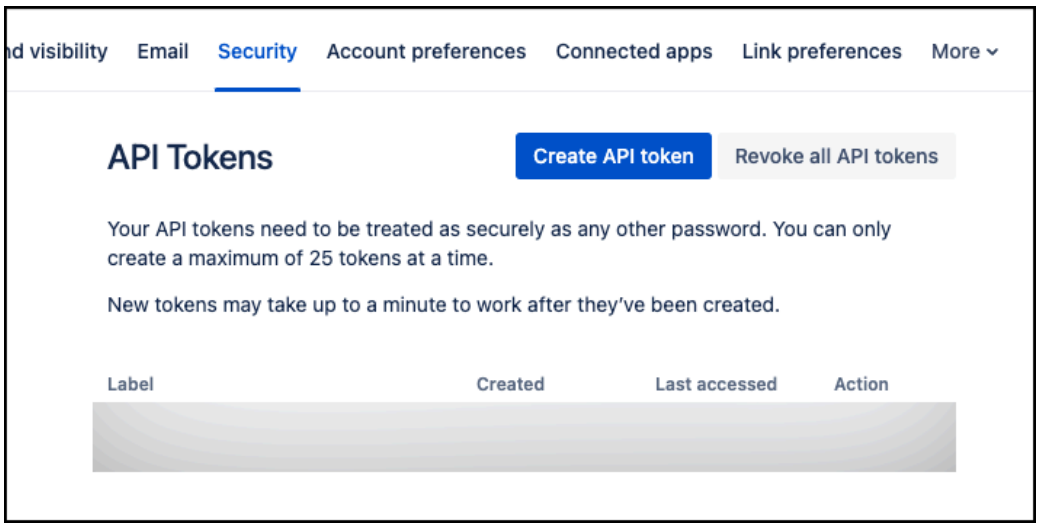
Basic authentication

You can connect Amazon Q to Confluence (Cloud) using basic authentication credentials. The following procedure gives you an overview of how to configure Confluence (Cloud) to connect to Amazon Q using basic authentication.

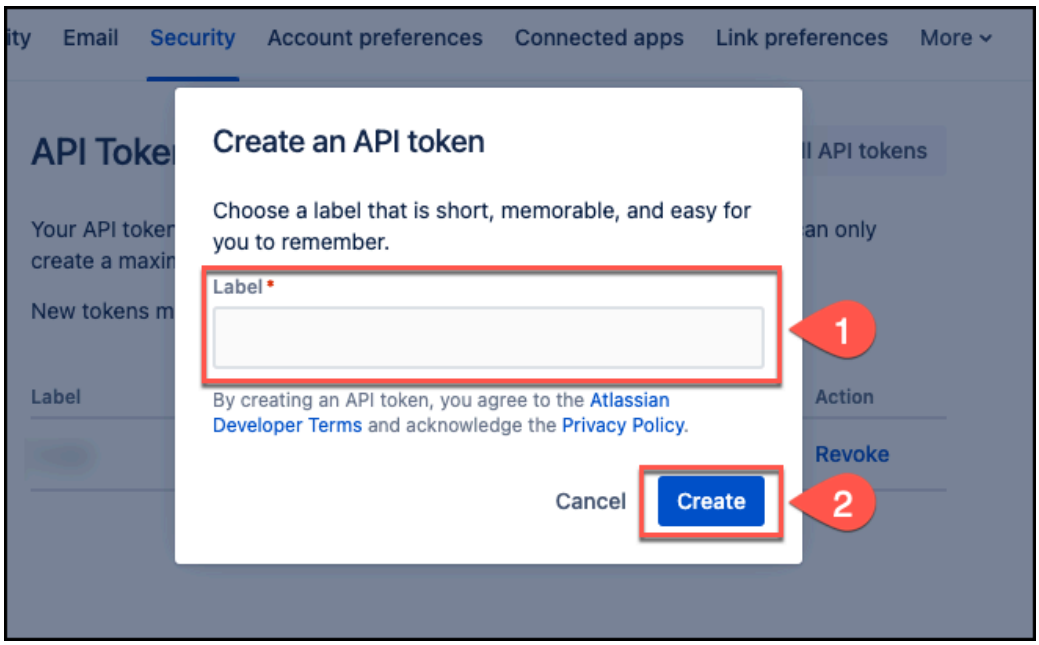
Configuring Confluence (Cloud) basic authentication for Amazon Q

1. Log in to your account from the Confluence (Cloud). Note the username you logged in with. You will need this later to connect to Amazon Q.
2. From your Confluence (Cloud) home page, note your Confluence (Cloud) URL from your Confluence browser URL. For example: *`https://example.atlassian.net`*. You will need this later to connect to Amazon Q.

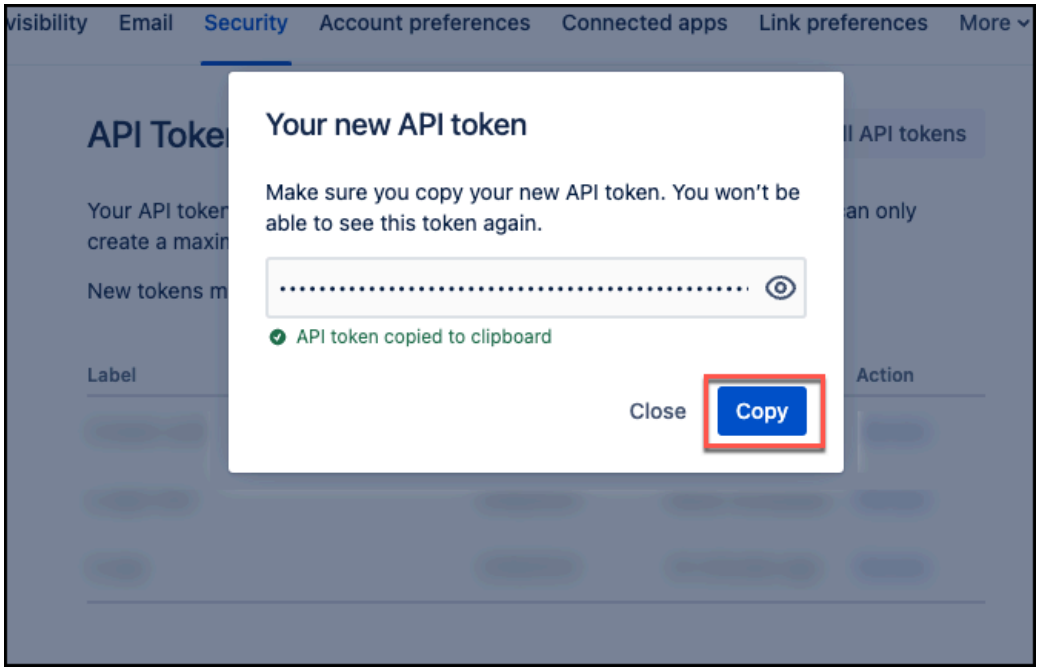
3. Then, go to Security page in Confluence (Cloud).
4. From the **API tokens** page, select **Create API token**.



5. In the **Create an API token** dialog box that opens, for **Label**, add a name for your API token. Then, select **Create**.



6. From the **Your new API token** dialog box, copy the API token and save it in a text editor of your choice. You can't retrieve the API token once you close the dialog box.



7. Select **Close**.

You now have the username, Confluence (Cloud) URL, and Confluence (Cloud) API token you need to connect to Amazon Q with basic authentication.

For more information, see Manage API tokens for your Atlassian account in Atlassian Support.

Atlassian Admin Authentication

To ensure Amazon Q can access all user and group information from your Confluence (Cloud) instance, you must provide Atlassian admin credentials. These credentials allow Amazon Q to sync user information regardless of individual email visibility settings.

Get your Atlassian admin credentials

1. Sign in to the Atlassian admin portal with administrator permissions.
2. Open the Administration app for your organization. The URL should look like: `https://admin.atlassian.com/o/{ORGANIZATION-UUID}/overview`
3. Choose **Settings**, then choose **API Keys**.
4. Choose **Create API key**.
5. Select all available scopes for the API key.

   Note that the Confluence APIs that fetch user and group information require full scope access.

6. Copy and save both the **Organization ID** and **API Key**. Note that API keys expire. Monitor the expiration date and update your data source credentials before the key expires.

Get your Directory ID

1. Use the Atlassian Admin Workspace API to get your Directory ID. Run the following command:

```
curl --request POST \
--url 'https://api.atlassian.com/admin/v2/orgs/{ORGANIZATION-ID}/workspaces' \
--header 'Authorization: Bearer {API-KEY}' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json'
```

2. In the API response, find the workspace entry that matches your Confluence Cloud instance. Look for `"type": "Confluence"`. Verify the workspace name matches your instance and then copy the directory value from the attributes section. If your instance isn't listed, use the pagination cursor in the `links.next` field to view additional pages.

```
curl --request POST \
--url 'https://api.atlassian.com/admin/v2/orgs/{ORGANIZATION-ID}/workspaces' \
--header 'Authorization: Bearer {API-KEY}' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--data '{"cursor": "{NEXT-PAGE-TOKEN}"}'
```

Update your Confluence data source

When creating or updating your Confluence Cloud data source, provide these three values in your AWS Secrets Manager secret:

1. Admin API Key
2. Organization ID
3. Directory ID

For more information about Atlassian admin API scopes, see Atlassian API scopes documentation.

For API details, see Atlassian Admin Workspace API reference.

OAuth 2.0 authentication

You can connect Amazon Q to Confluence (Cloud) using OAuth 2.0 authentication credentials. The following procedures give you an overview of how to configure Confluence (Cloud) to connect to Amazon Q using OAuth 2.0 authentication.

Steps to configure Confluence (Cloud) OAuth 2.0 authentication

- Step 1: Retrieving username and Confluence (Cloud) URL
- Step 2: Configuring an OAuth 2.0 app integration
- Step 3: Retrieving Confluence (Cloud) client ID and client Secret
- Step 4: Generating an Confluence (Cloud) access token
- Step 5: Generating a Confluence (Cloud) refresh token
- Step 6: Generating a new Confluence (Cloud) access token using a refresh token

Step 1: Retrieving username and Confluence (Cloud) URL

To connect Confluence (Cloud) to Amazon Q, you need your Confluence (Cloud) username and your Confluence (Cloud) URL. The following procedure shows you how to retrieve these.

Retrieving username and Confluence (Cloud) URL

1. Log in to your account from the Confluence (Cloud). Note the username you logged in with. You will need this later to connect to Amazon Q.
2. From your Confluence (Cloud) home page, note your Confluence (Cloud) URL from your Confluence browser URL. For example: *`https://example.atlassian.net`*. You will need this later to both configure your OAuth 2.0 token and connect to Amazon Q.

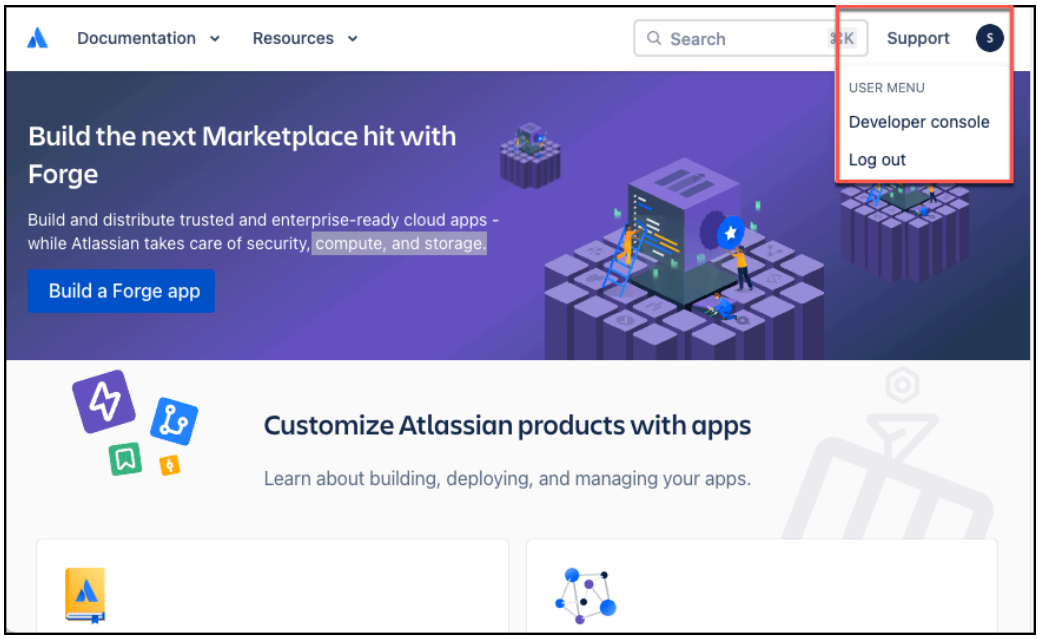
Step 2: Configuring an OAuth 2.0 app integration

To connect Confluence (Cloud) to Amazon Q using OAuth 2.0 authentication, you need to create a Confluence (Cloud) OAuth 2.0 app with the necessary permissions. The following procedure shows you how to create this.

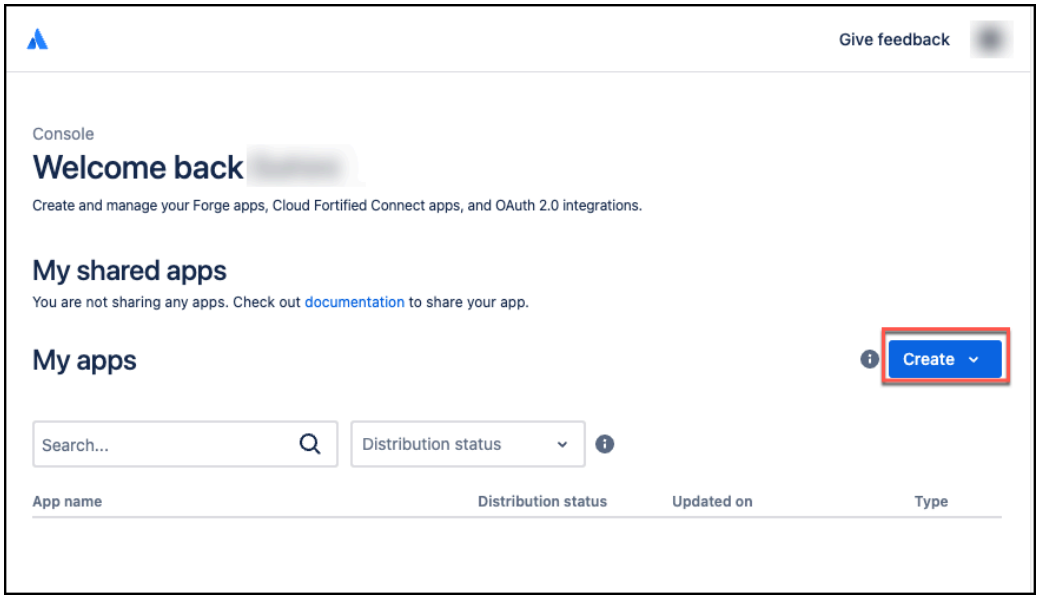
Configuring an OAuth 2.0 app integration

1. Log in to your account from the Atlassian Developer page.

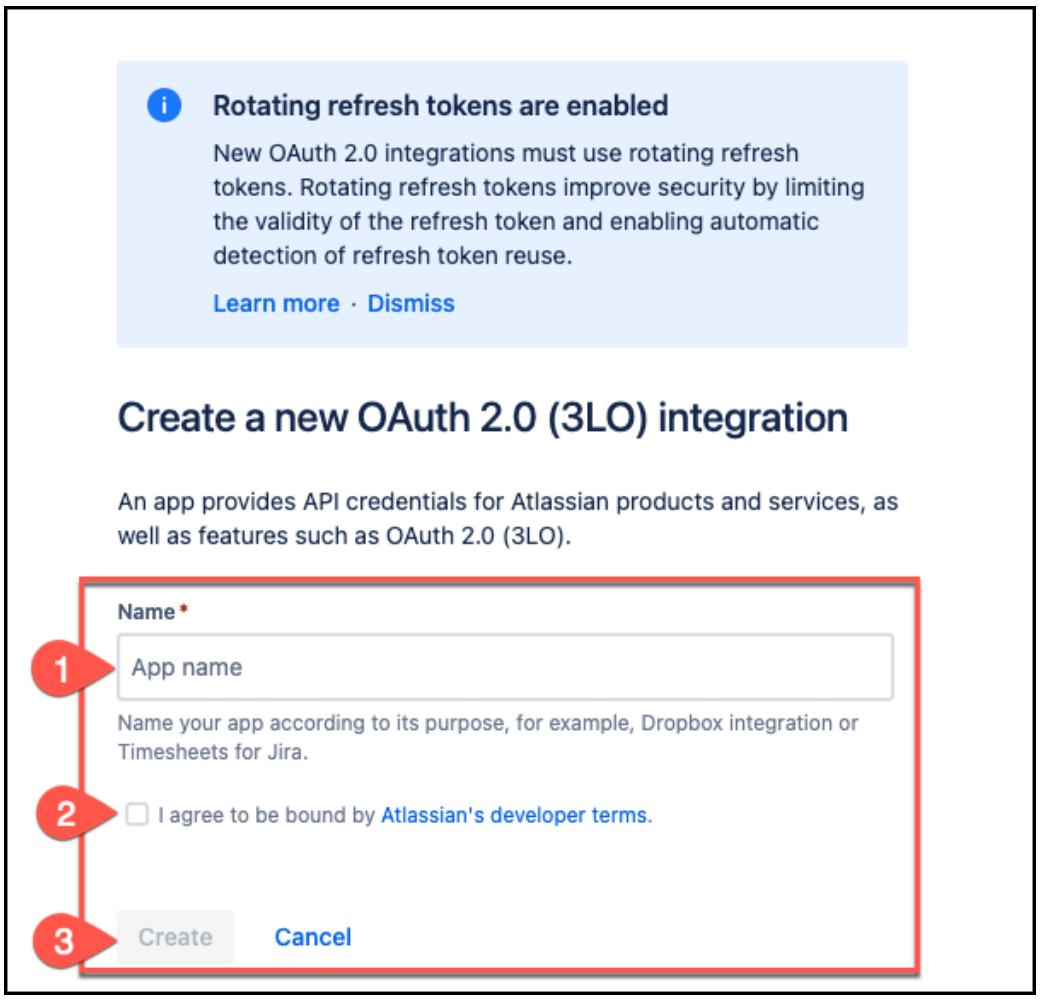
2. Select the profile icon from the top-right corner. Then, from the dropdown menu that opens, select **Developer Console**.



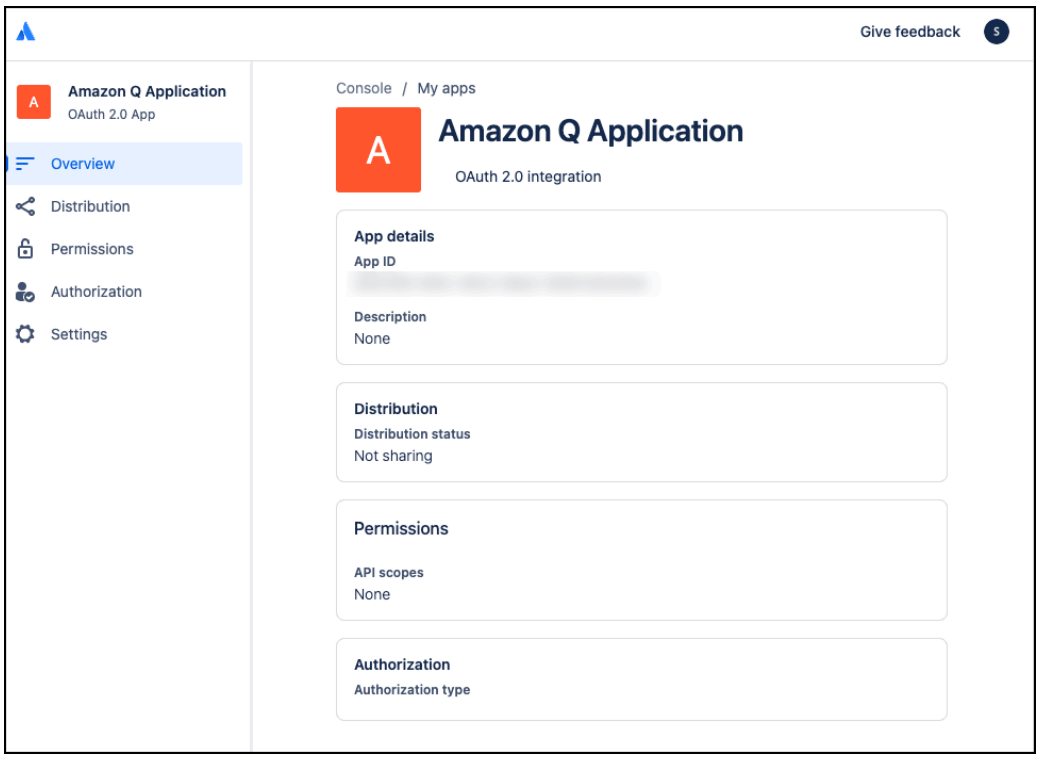
3. From the **Welcome** page, select **Create** and then select **OAuth 2.0 integration**.



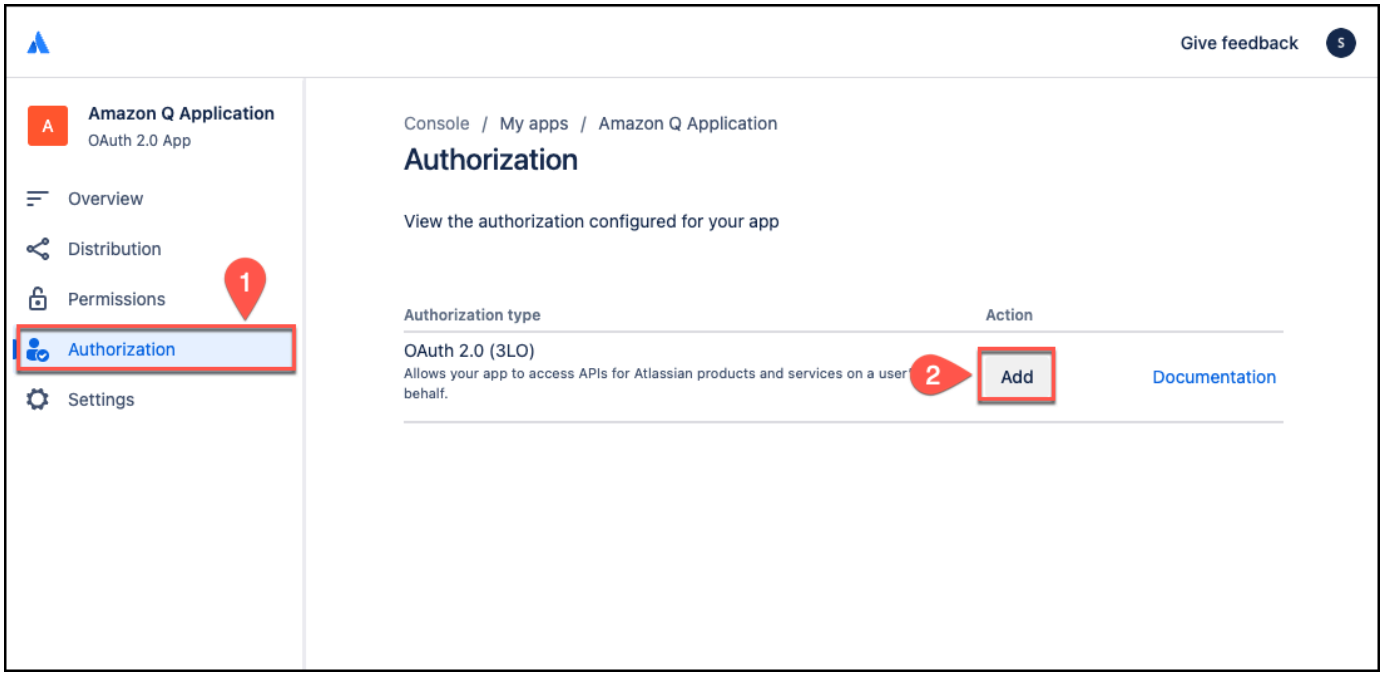
4. On the **Create a new OAuth 2.0 (3LO) integration** page, for **Name**, enter a name for the OAuth 2.0 application you are creating. Then, select the **I agree to be bound by Atlassian's developer terms** checkbox, and select **Create**.



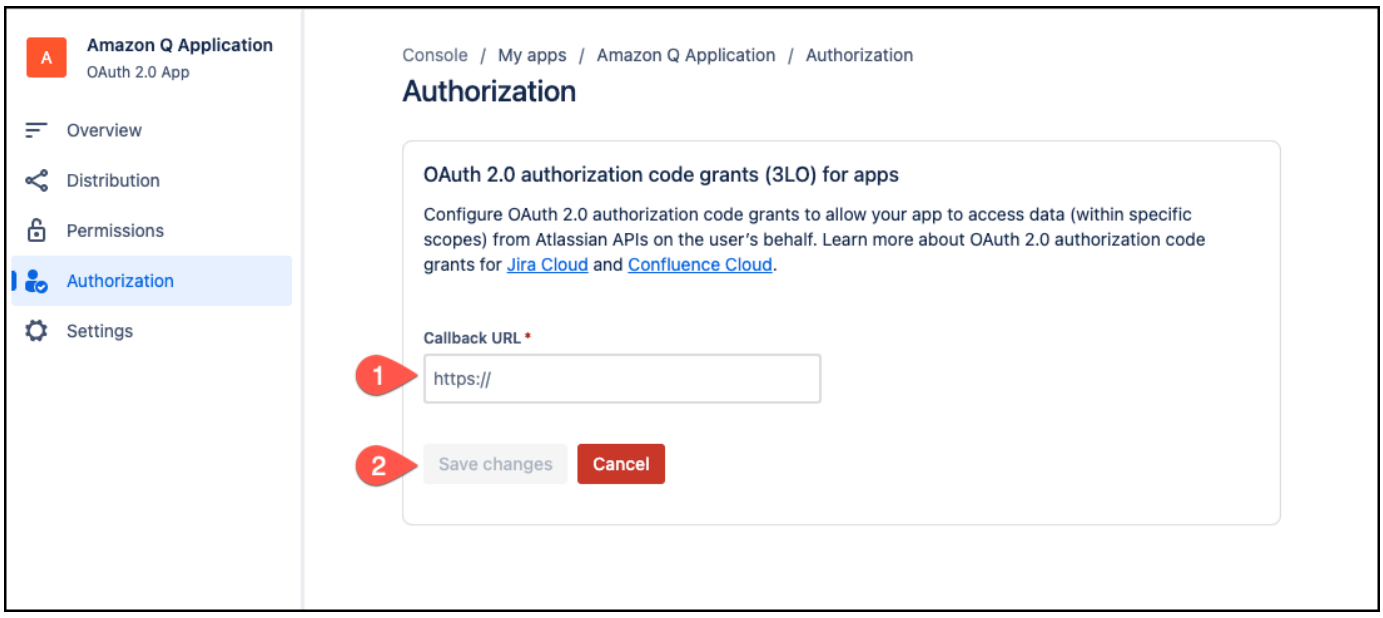
The console will display a summary page outlining the details of the OAuth 2.0 app created.



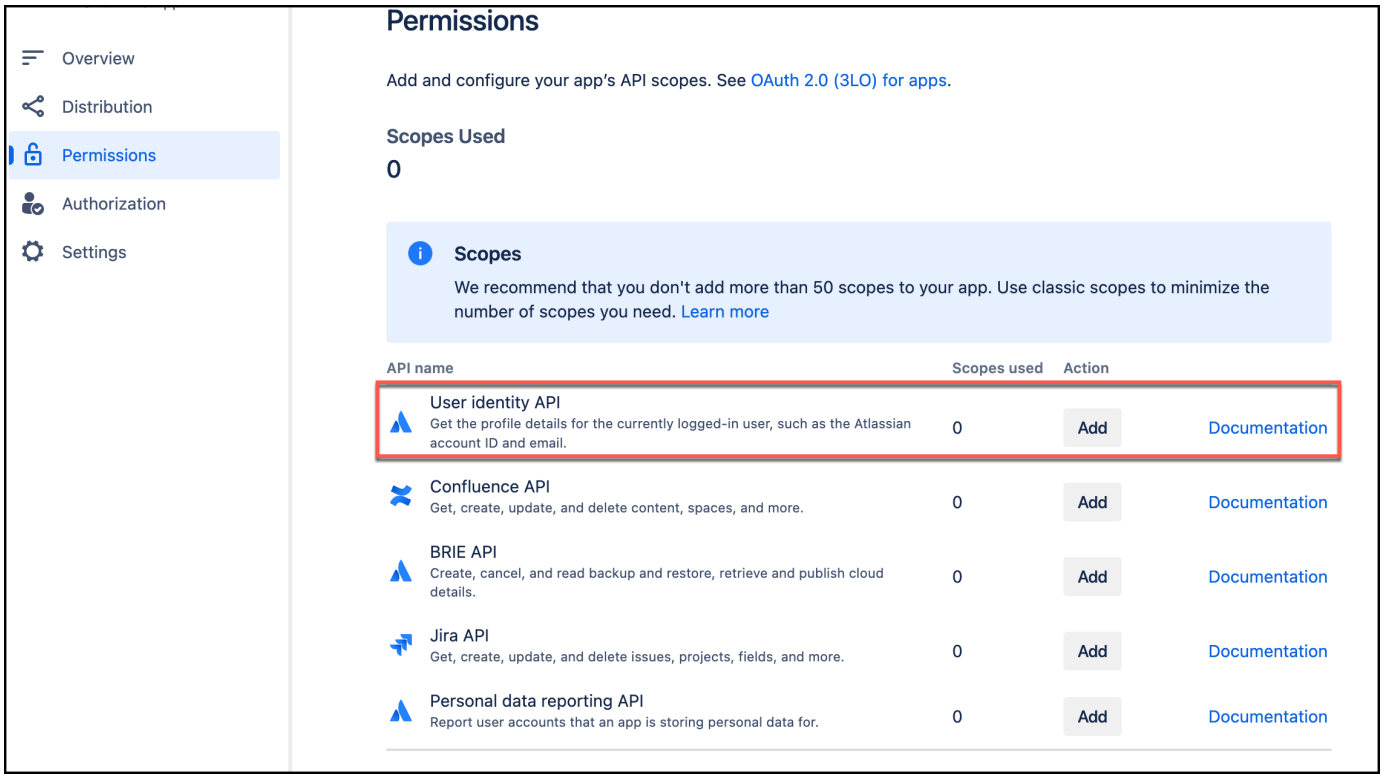
5. From the left navigation menu, choose **Authorization**.
6. From the **Authorization** page, choose **Add** to add **OAuth 2.0 (3LO)** to your app.



7. On the **OAuth 2.0 authorization code grants (3LO) for apps**, enter the Confluence (Cloud) URL you copied as the **Callback URL** and then choose **Save changes**.



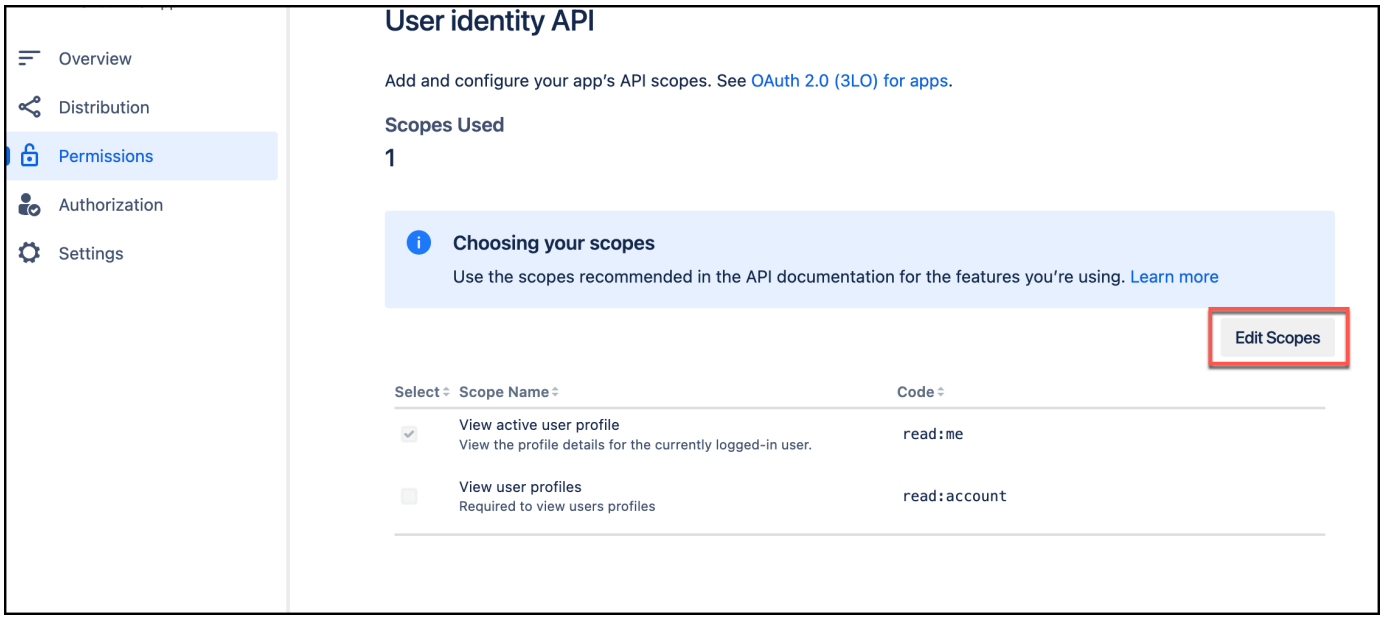
8. From the **Authorization URL generator** section that appears, choose **Add APIs** to add APIs to your app. This will redirect you to the **Permissions** page.
9. On the **Permissions** page, for **Scopes**, navigate to **User Identity API**. Select **Add**, and then select **Configure**.



10. On the **User Identity API** page, choose **Edit Scopes**, and the add the following `read` scopes:

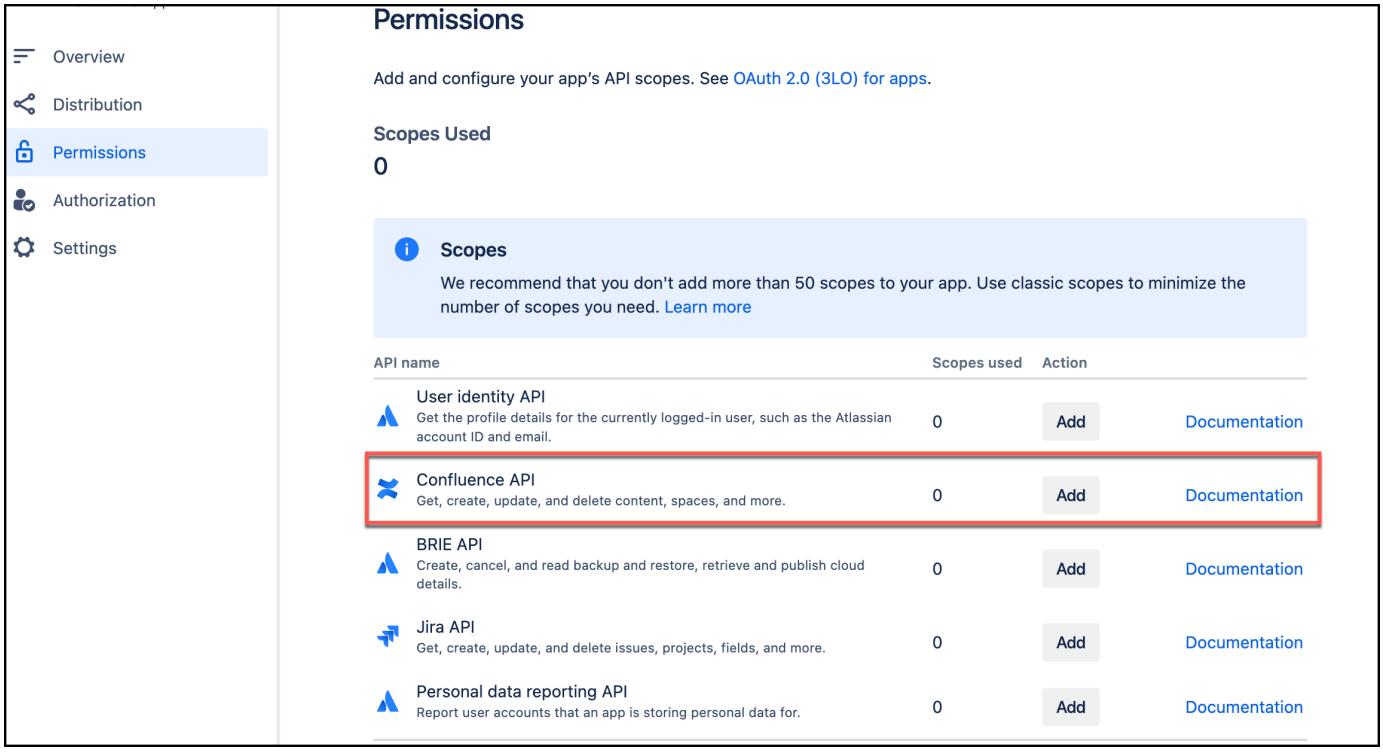
    - **`read:me`** – View active user profile

- **`read:account`** – View user profiles

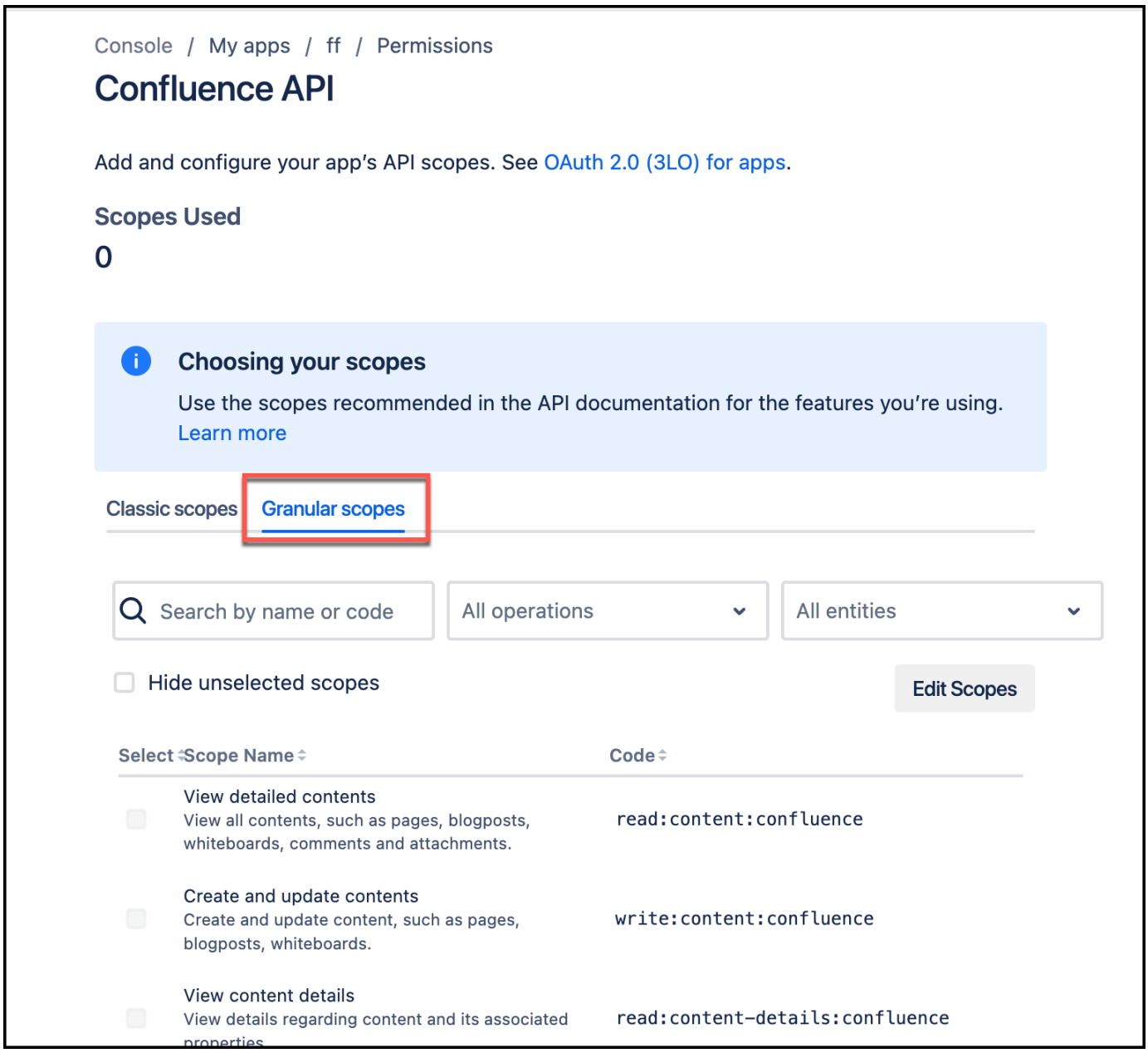


Then, select **Save**.

11. Return to the **Permissions** page. From **Scopes**, navigate to **Confluence API**. Select **Add**, and the select **Configure**.



12. Navigate to the **Granular scopes** page.



Then, choose **Edit Scopes**, and the add the following `read` scopes:

- **`read:content:confluence`** – View detailed contents
- **`read:content-details:confluence`** – View content details
- **`read:space-details:confluence`** – View space details
- **`read:audit-log:confluence`** – View audit records
- **`read:page:confluence`** – View pages
- **`read:attachment:confluence`** – View and download content attachments

- **`read:blogpost:confluence`** – View blogposts
- **`read:custom-content:confluence`** – View custom content
- **`read:comment:confluence`** – View comments
- **`read:template:confluence`** – View content templates
- **`read:label:confluence`** – View labels
- **`read:watcher:confluence`** – View content watchers
- **`read:group:confluence`** – View groups
- **`read:relation:confluence`** – View entity relationships
- **`read:user:confluence`** – View user details
- **`read:configuration:confluence`** – View Confluence settings
- **`read:space:confluence`** – View space details
- **`read:space.permission:confluence`** – View space permissions
- **`read:space.property:confluence`** – View space properties
- **`read:user.property:confluence`** – View user properties
- **`read:space.setting:confluence`** – View space settings
- **`read:analytics.content:confluence`** – View analytics for content
- **`read:content.permission:confluence`** – Check content permissions
- **`read:content.property:confluence`** – View content properties
- **`read:content.restriction:confluence`** – View content restrictions
- **`read:content.metadata:confluence`** – View content summaries
- **`read:inlinetask:confluence`** – View tasks
- **`read:task:confluence`** – View tasks
- **`read:permission:confluence`** – View content restrictions and space permissions
- **`read:whiteboard:confluence`** – View whiteboards
- **`read:app-data:confluence`** – Read app data
- *(Optional)* **`read:database:confluence`** – Read database
- *(Optional)* **`read:embed:confluence`** – Read embeddings
- *(Optional)* **`read:folder:confluence`** – Read folders
- *(Optional)* **`read:email-address:confluence`** – Read email addresses

Then, select **Save**.

For more information, see Implementing OAuth 2.0 (3LO) and Determining the scopes required for an operation in Atlassian Developer.

Atlassian Admin Authentication

To ensure Amazon Q can access all user and group information from your Confluence (Cloud) instance, you must provide Atlassian admin credentials. These credentials allow Amazon Q to sync user information regardless of individual email visibility settings.

Get your Atlassian admin credentials

1. Sign in to the Atlassian admin portalwith administrator permissions.
2. Open the Administration app for your organization. The URL should look like: `https://admin.atlassian.com/o/{ORGANIZATION-UUID}/overview`
3. Choose **Settings**, then choose **API Keys**.
4. Choose **Create API key**\
5. Select all available scopes for the API key.

   Note that the Confluence APIs that fetch user and group information require full scope access.
6. Copy and save both the **Organization ID** and **API Key**. Note that API keys expire. Monitor the expiration date and update your data source credentials before the key expires.

Get your Directory ID

1. Use the Atlassian Admin Workspace API to get your Directory ID. Run the following command:

```
curl --request POST \
--url 'https://api.atlassian.com/admin/v2/orgs/{ORGANIZATION-ID}/workspaces' \
--header 'Authorization: Bearer {API-KEY}' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json'
```

2. In the API response, find the workspace entry that matches your Confluence Cloud instance. Look for `"type": "Confluence"`. Verify the workspace name matches your instance and then copy the directory value from the attributes section. If your instance isn't listed, use the pagination cursor in the `links.next` field to view additional pages.

```
curl --request POST \
--url 'https://api.atlassian.com/admin/v2/orgs/{ORGANIZATION-ID}/workspaces' \
--header 'Authorization: Bearer {API-KEY}' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--data '{"cursor": "{NEXT-PAGE-TOKEN}"}'
```

Creating your Confluence data source

When creating your Confluence Cloud data source, provide these three values in your AWS Secrets Manager secret:

1. Admin API Key
2. Organization ID
3. Directory ID

For more information about Atlassian admin API scopes, see Atlassian API scopes documentation.

For API details, see Atlassian Admin Workspace API reference.

Updating your Confluence data source

To update an existing Confluence Cloud data source with new admin credentials, add the following key pairs to your AWS Secrets Manager secret:

1. adminApiKey, {Admin API Key}
2. organizationId, {Organization ID}
3. directoryId, {Directory ID}

For more information about Atlassian admin API scopes, see Atlassian API scopes documentation.

For API details, see Atlassian Admin Workspace API reference.

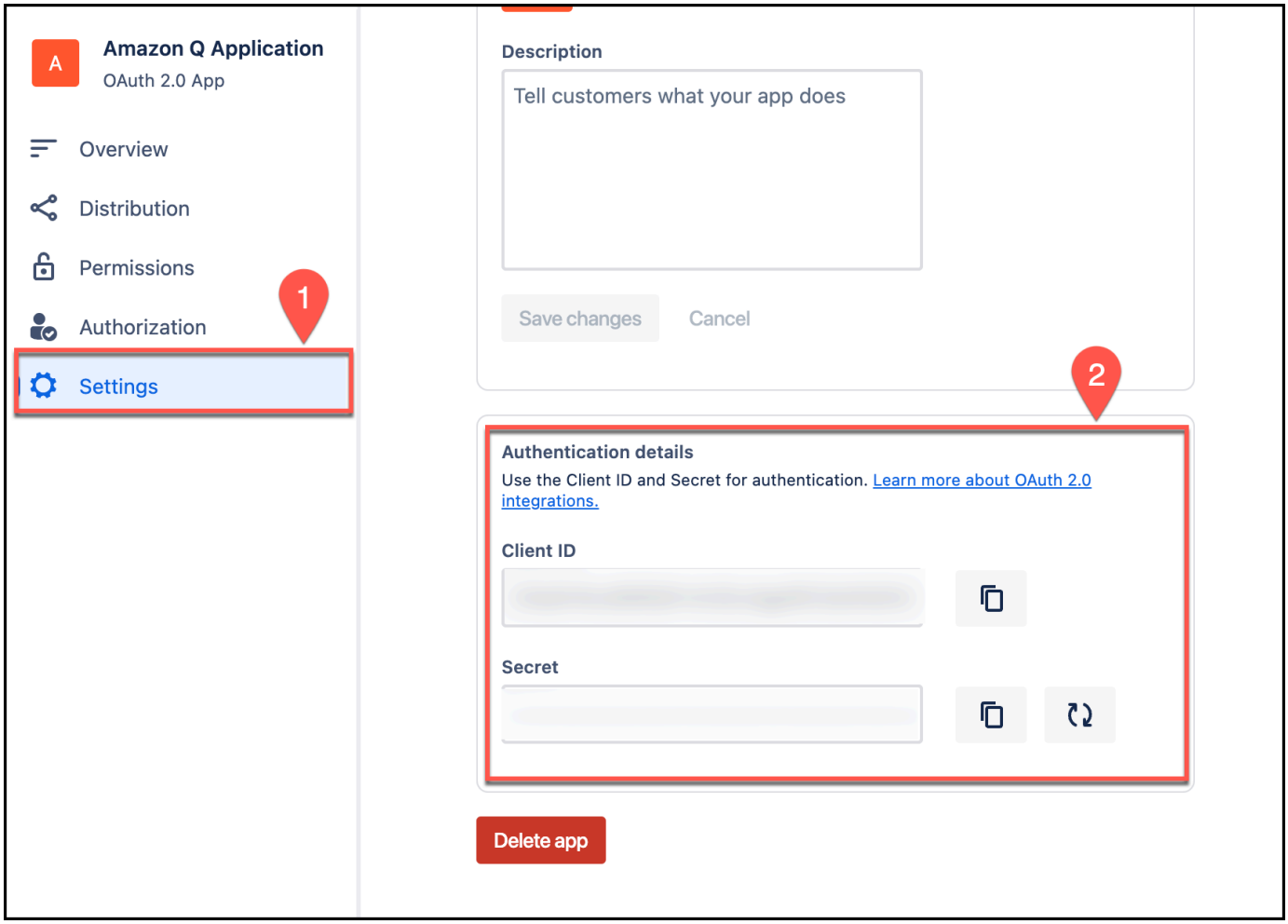
Step 3: Retrieving Confluence (Cloud) client ID and client Secret

To connect Confluence (Cloud) to Amazon Q using OAuth 2.0 authentication, you need to provide a Confluence (Cloud) client ID and client secret. The following procedure shows you how to retrieve these.

> **Note**
>
> You must create an OAuth 2.0 app before you can retrieve the client ID and client secret. See Configuring an OAuth 2.0 app integration for more details.

Retrieving Confluence (Cloud) client ID and client secret

- From the left navigation menu, choose **Settings**. Then, scroll down to **Authentication details** section and copy and save the following in a text editor of your choice:
  - Client ID – You will enter this as **App key** in the Amazon Q console.
  - Client Secret – You will enter this as **App secret** in the Amazon Q console.



You will need these to generate your Confluence (Cloud) OAuth 2.0 token and also to connect Amazon Q to Confluence (Cloud).

For more information, see Implementing OAuth 2.0 (3LO) and Determining the scopes required for an operation in Atlassian Developer.

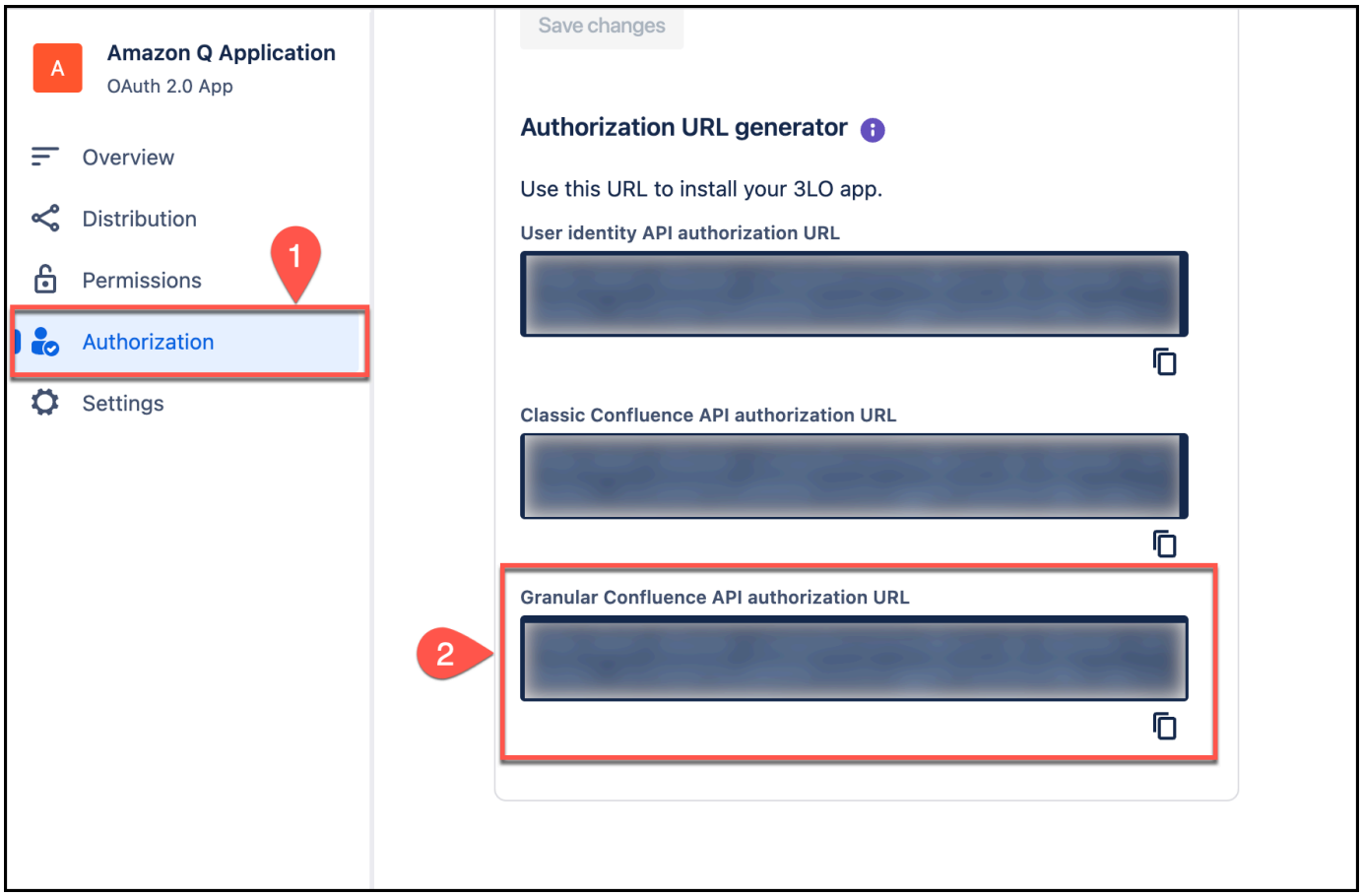
Step 4: Generating an Confluence (Cloud) access token

To connect Confluence (Cloud) to Amazon Q, you need to generate an access token. The following procedure outlines how to generate an access token in Confluence (Cloud).

Generating your Confluence (Cloud) access token

1. Log in to your account from the Atlassian Developer page.
2. Open the OAuth 2.0 app you want to generate a refresh token for.

3. From the left navigation menu, choose **Authorization** again. Then, for **OAuth 2.0 (3LO)**, choose **Configure**.
4. From the **Authorization** page, from **Authorization URL generator**, from **Granular Confluence API authorization URL**, copy the URL and save it in a text editor of your choice.



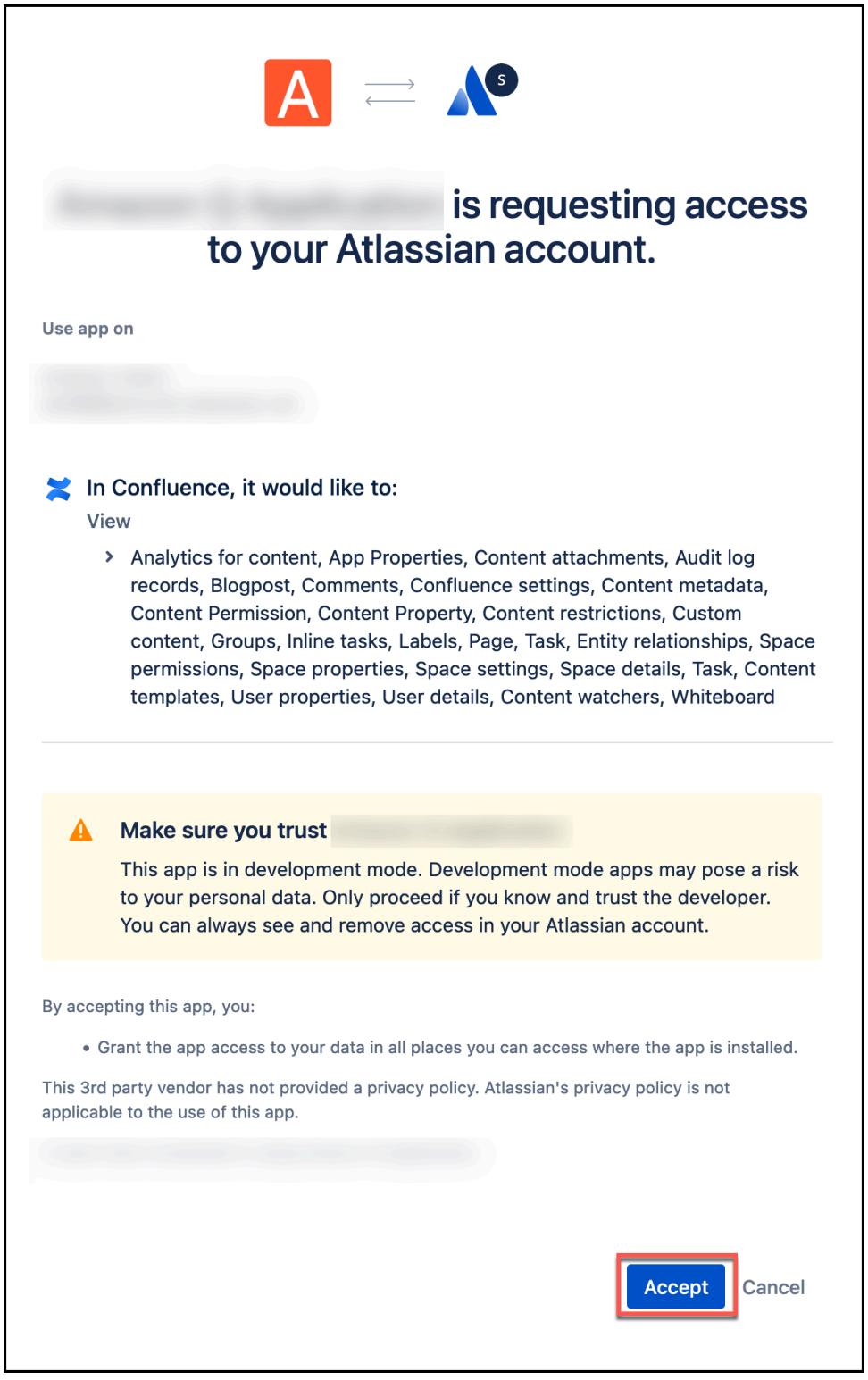
The URL is of the following format:

```
https://auth.atlassian.com/authorize?
audience=api.atlassian.com
&client_id=YOUR_CLIENT_ID
&scope=REQUESTED_SCOPE%20REQUESTED_SCOPE_TWO
&redirect_uri=https://YOUR_APP_CALLBACK_URL
&state=YOUR_USER_BOUND_VALUE
&response_type=code
&prompt=consent
```

5. In the saved authorization URL, update the `state=${YOUR_USER_BOUND_VALUE}` parameter value to any text of your choice. For example, `state=sample_text`.

For more information, see What is the state parameter used for? in Atlassian Support.

6. Open a web browser of your choice. Then, paste the authorization URL you copied into the browser URL. On the page that opens up, make sure everything is correct and then select **Accept**.



You will be returned to your Confluence (Cloud) home page.

7. Copy the URL of the Confluence (Cloud) home page and save it in a text editor of your choice. The URL contains the authorization code for your application. You will need this code

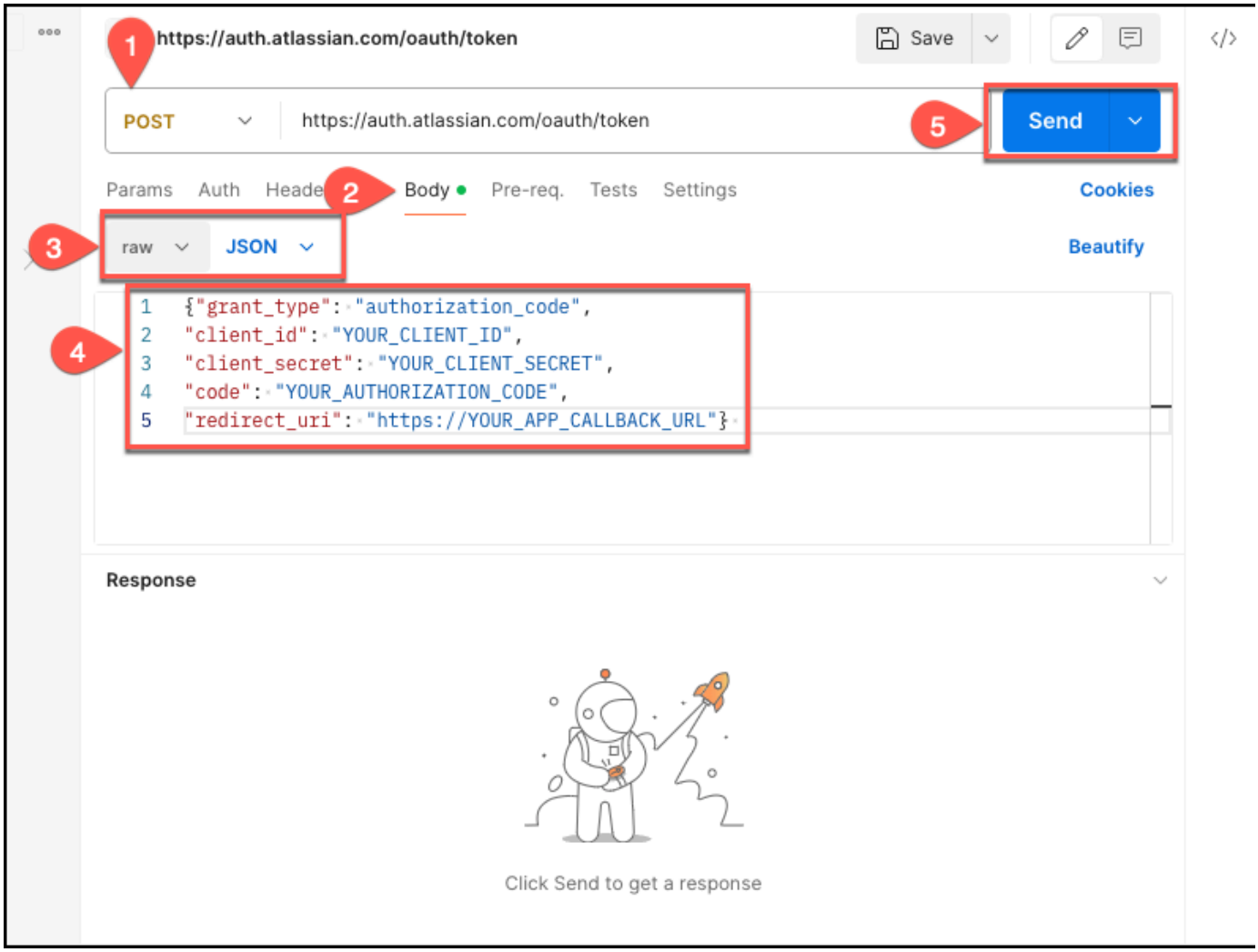
to generate your Confluence (Cloud) access token. The whole section after `code=` is the authorization code.

8. Navigate to Postman.

   If you don't have Postman, you can also choose to use cURL to generate a Confluence (Cloud) access token. Use the following cURL command to do so:

```
curl --location 'https://auth.atlassian.com/oauth/token' \
--header 'Content-Type: application/json' \
--data '{"grant_type": "authorization_code",
"client_id": "YOUR_CLIENT_ID",
"client_secret": "YOUR_CLIENT_SECRET",
"code": "AUTHORIZATION_CODE",
"redirect_uri": "YOUR_CALLBACK_URL"}'
```

9. On the Postman home page, select POST as the method, and then enter the following URL in the **Enter URL or paste text** box: `https://auth.atlassian.com/oauth/token`.
10. Then, select **Body** from the menu, and select **raw JSON**.



11. In the text box, enter the following code extract, replacing the fields with your credential values:

```
{"grant_type": "authorization_code",
"client_id": "YOUR_CLIENT_ID",
"client_secret": "YOUR_CLIENT_SECRET",
"code": "YOUR_AUTHORIZATION_CODE",
"redirect_uri": "https://YOUR_APP_CALLBACK_URL"}
```

12. Then, select **Send**. If everything is configured correctly, Postman will return an `access-token`. Copy the access token and save it using a text editor of your choice. You will need it to connect Confluence (Cloud) to Amazon Q.

For more information, see Implementing OAuth 2.0 (3LO) in Atlassian Developer.

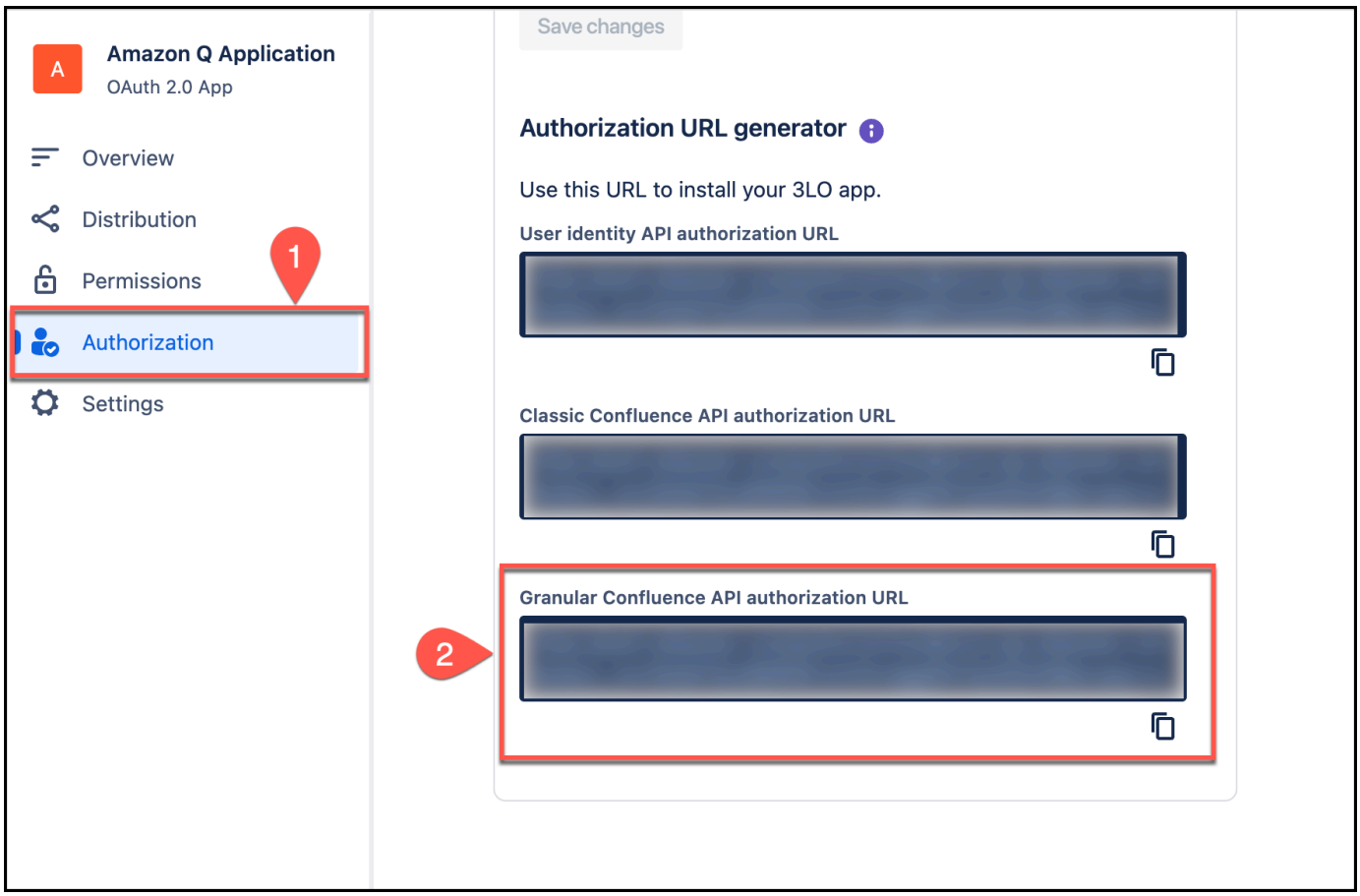
Step 5: Generating a Confluence (Cloud) refresh token

The access token you use to connect Confluence (Cloud) to Amazon Q using OAuth 2.0 authentication expires after 1 hour. When it does, you can either repeat the whole authorization process and generate a new access token. Or, you can choose to generate a refresh token. You can use the refresh token to regenerate a new access token when an existing access token expires.

To do this, you add a `%20offline_access` parameter to the end of the `scope` value in the authorization URL you used to generate your access token. The following procedure shows you how to generate a refresh token.

Generating an Confluence (Cloud) refresh token

1. Log in to your account from the Atlassian Developer page.
2. Open the OAuth 2.0 app you want to generate a refresh token for.
3. From the left navigation menu, choose **Authorization** again. Then, for **OAuth 2.0 (3LO)**, choose **Configure**.
4. From the **Authorization** page, from **Authorization URL generator**, from **Granular Confluence API authorization URL**, copy the URL and save it in a text editor of your choice.



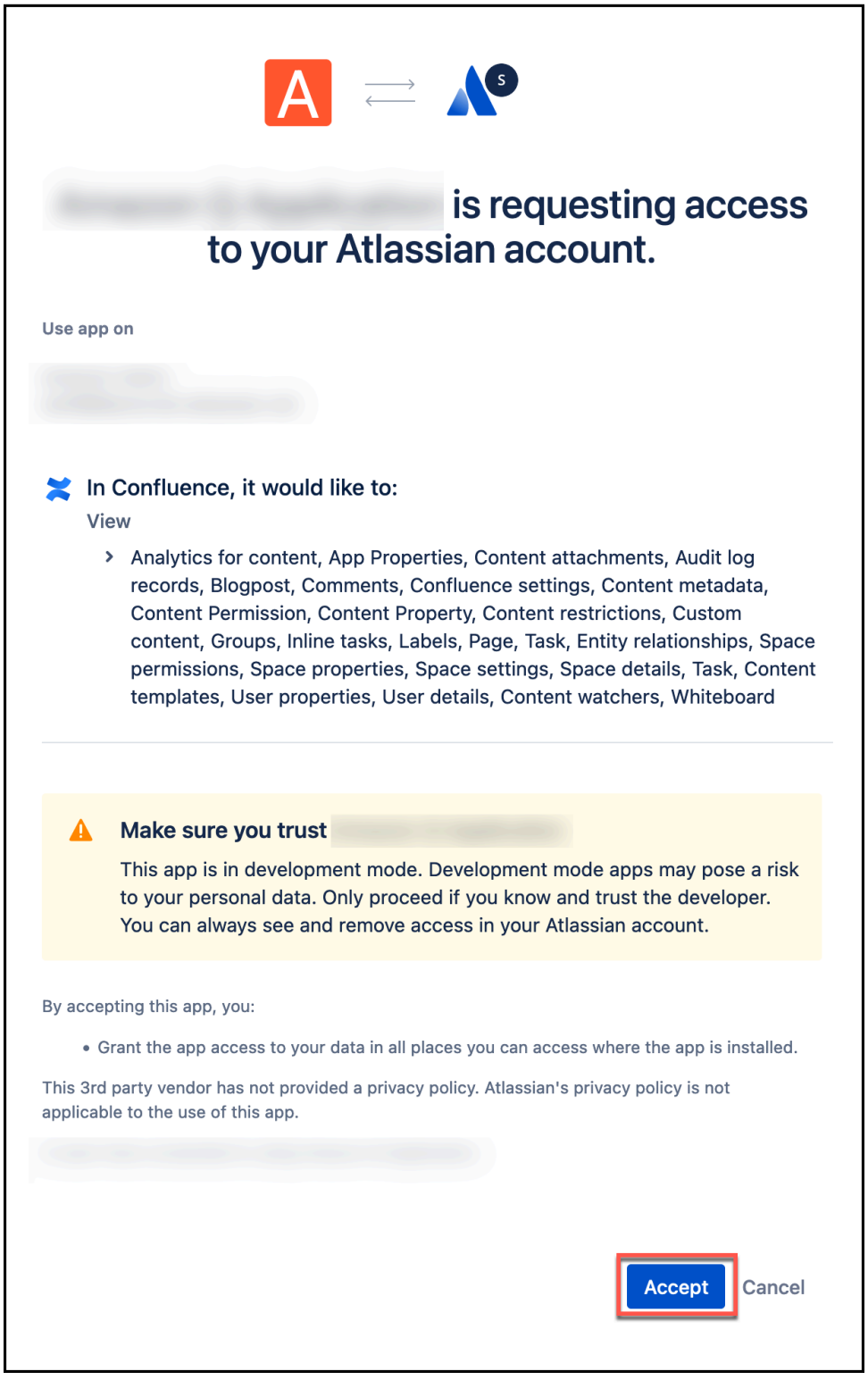
5. In the saved authorization URL, update the `state=${YOUR_USER_BOUND_VALUE}` parameter value to any text of your choice. For example, `state=sample_text`.

   For more information, see What is the state parameter used for? in Atlassian Support.

6. Then, add the following text at the end of the `scope` value in your authorization URL: `%20offline_access` and copy it. For example:

```
https://auth.atlassian.com/authorize?
audience=api.atlassian.com
&client_id=YOUR_CLIENT_ID
&scope=REQUESTED_SCOPE%20REQUESTED_SCOPE_TWO%20offline_access
&redirect_uri=https://YOUR_APP_CALLBACK_URL
&state=YOUR_USER_BOUND_VALUE
&response_type=code
&prompt=consent
```

7. Open a web browser of your choice and paste the modified authorization URL you copied into the browser URL. On the page that opens up, make sure everything is correct and then select **Accept**.



You will be returned to the Confluence (Cloud) console.

8. Copy the URL of the Confluence (Cloud) home page and save it in a text editor of your choice. The URL contains the authorization code for your application. You will need this code

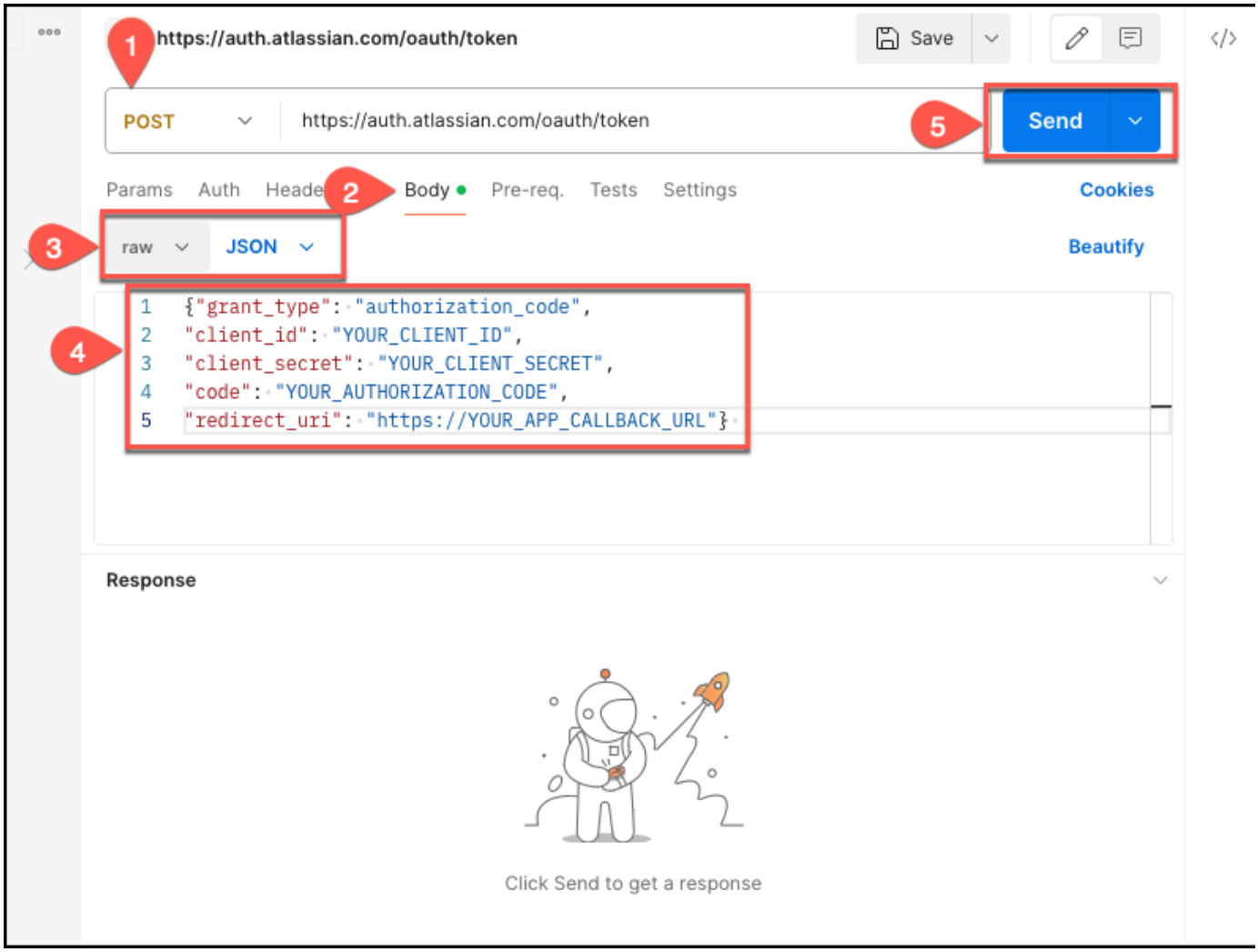
to generate your Confluence (Cloud) refresh token. The whole section after `code=` is the authorization code.

9. Navigate to Postman.

   If you don't have Postman, you can also choose to use cURL to generate a Confluence (Cloud) access token. Use the following cURL command to do so:

```
curl --location 'https://auth.atlassian.com/oauth/token' \
--header 'Content-Type: application/json' \
--data '{"grant_type": "authorization_code",
"client_id": "YOUR CLIENT ID",
"client_secret": "YOUR CLIENT SECRET",
"code": "AUTHORIZATION CODE",
"redirect_uri": "YOUR CALLBACK URL"}'
```

10. On the Postman home page, select POST as the method, and then enter the following URL in the **Enter URL or paste text** box: `https://auth.atlassian.com/oauth/token`.
11. Then, select **Body** from the menu, and select **raw JSON**.



12. In the text box, enter the following code extract, replacing the fields with your credential values:

```
{"grant_type": "authorization_code",
"client_id": "YOUR_CLIENT_ID",
"client_secret": "YOUR_CLIENT_SECRET",
"code": "YOUR_AUTHORIZATION_CODE",
"redirect_uri": "https://YOUR_APP_CALLBACK_URL"}
```

13. Then, select **Send**. If everything is configured correctly, Postman will return an `refresh-token`.

    Copy the refresh token and save it using a text editor of your choice. You will need it to connect Confluence (Cloud) to Amazon Q.

For more information, see Implementing a Refresh Token Flow in Atlassian Developer.

Step 6: Generating a new Confluence (Cloud) access token using a refresh token

You can use the refresh token you generated to create a new access token-refresh token pair when an existing access token expires. The following procedure shows you how to generate a refresh token.

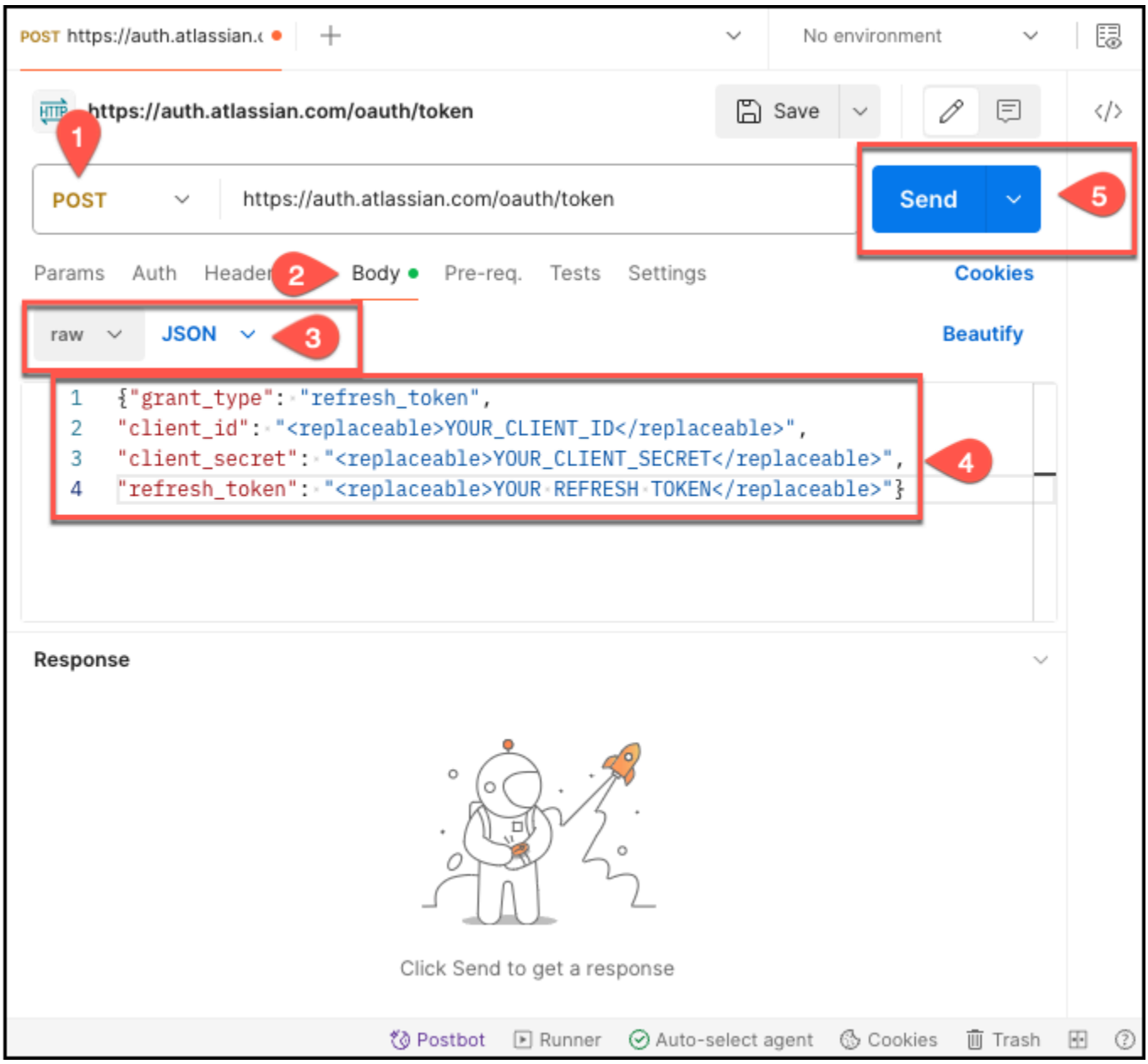
Generating an Confluence (Cloud) access token-refresh token pair

1. Copy the refresh token you generated following the steps in Step 5: Generating a Confluence (Cloud) refresh token.
2. Navigate to Postman.

   If you don't have Postman, you can also choose to use cURL to generate a new Confluence (Cloud) access token. Use the following cURL command to do so:

   ```
   curl --location 'https://auth.atlassian.com/oauth/token' \
   --header 'Content-Type: application/json' \
   --data '{"grant_type": "refresh_token",
   "client_id": "YOUR_CLIENT_ID",
   "client_secret": "YOUR_CLIENT_SECRET",
   "refresh_token": "YOUR_REFRESH_TOKEN"}'
   ```

3. On the Postman home page, select POST as the method, and then enter the following URL in the **Enter URL or paste text** box: `https://auth.atlassian.com/oauth/token`.
4. Then, select **Body** from the menu, and select **raw JSON**.



5. In the text box, enter the following code extract, replacing the fields with your credential values:

```
{"grant_type": "refresh_token",
"client_id": "YOUR_CLIENT_ID",
"client_secret": "YOUR_CLIENT_SECRET",
"refresh_token": "YOUR REFRESH TOKEN"}
```

6. Then, select **Send**. If everything is configured correctly, Postman will return a new access token-refresh token pair in the following format:

```
{
"access_token": "string,
"expires_in": "expiry time of access_token in second",
"scope": "string",
"refresh_token": "string"
}
```

For more information, see Implementing a Refresh Token Flow and How do I get a new access token, if my access token expires or is revoked? in Atlassian Developer.

How Amazon Q works with Confluence (Cloud) access and refresh tokens

The following are important points to note about using Confluence (Cloud) access and refresh tokens with Amazon Q:

- If a Confluence (Cloud) access token-refresh token pair you use to connect to Amazon Q are expired or invalid, the Amazon Q sync process fails. If this happens, you need to generate and provide a new pair of tokens.
- If your access token is valid but you have an invalid refresh token, Amazon Q will sync data until the access token expires (up to 1 hour). After the access token expires, you won't be able to re-generate an access token-refresh token pair using the expired refresh token. When both access token and refresh token expire, the Amazon Q Confluence (Cloud) data source connector stops syncing.
- If an access token expires during the Confluence (Cloud) connector sync process, the connector internally regenerates a new pair of tokens using the existing refresh token (if the provided refresh token is valid). After regenerating the new pair of tokens, the old pair is invalidated by Confluence (Cloud) and can't be re-used. To sync documents again after the connector auto-regenerates tokens, you must provide a new access token-refresh token pair.
- If you use OAuth, select **Rotate secret** if you want Amazon Q to rotate the secret automatically so that you don’t have to manually update the secret every time before you sync.
- As a best practice, use Confluence (Cloud) OAuth and the **Rotate secret** feature for the Amazon Q connector.

Checking Confluence (Cloud) connectivity

Before you sync your Confluence (Cloud) data source connector after configuring it, we recommend you check the connection between Amazon Q Business and Confluence (Cloud). The following are the cURL commands you need to check Confluence (Cloud) connectivity.

Topics

- Checking basic authentication connectivity

Checking basic authentication connectivity

To check connectivity for a Confluence (Cloud) data source connector using basic authentication, use the following cURL command:

```
curl --location 'https://<confluence_host-url>/wiki/rest/api/user/current'
--header 'Authorization: Basic <base64(email:api_token)>'
```

If your data source is connected as expected, the JSON response should resemble the following:

```
{
    "type": "known",
    "accountId": "accountId",
    "accountType": "atlassian",
    "email": "email",
    "publicName": "Administrator",
    "profilePicture": {
        "path": "/wiki/aa-avatar/<accountId>",
        "width": 48,
        "height": 48,
        "isDefault": false
    },
    "displayName": "Administrator",
    "isExternalCollaborator": false,
    "_expandable": {
        "operations": "",
        "personalSpace": ""
    },
    "_links": {
        "self": "https://<host_url>/wiki/rest/api/user?accountId=<accountId>",
        "base": "https://<host_url>/wiki",
        "context": "/wiki"
```

```
    }
}
```

If your Confluence (Cloud) connector is not connected correctly, you will see the following error:

- CNF-5123: The profile value is invalid. Try again after sometime.

To troubleshoot the issue, check your Confluence (Cloud) URL and make sure it's correct.

Connecting Amazon Q Business to Confluence (Cloud) using the console

The following procedure outlines how to connect Amazon Q Business to Confluence (Cloud) using the AWS Management Console.

Connecting Amazon Q to Confluence (Cloud)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Confluence** data source to your Amazon Q application.
5. Then, on the **Confluence (Cloud)** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, enter the following information:

   a. In **Source**, for **Hosting Method**, choose **Confluence Cloud**.

   b. **Confluence URL** – Enter the Confluence host URLs. The format for the host URL that you enter is *`https://example.atlassian.net`*.

> **Important**
>
> If you change or update your Confluence (Cloud) data source URL, you also need to update your Secrets Manager secret to ensure a secure connection.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
9. For **Authentication** – Choose between **Basic authentication** and **Oauth 2.0 authentication**, based on your use case.
10. **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your Confluence authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens. Enter the following information in the window:

    a. **Secret name** – A name for your secret.

    b. If using **Basic Authentication** – Enter the **Secret name User name**, and **Password** (Confluence API token) that you generated and downloaded from your Confluence account.

    If using **OAuth2.0 Authentication** – Enter the **Secret name**, **App key**, **App secret**, **Access token**, and **Refresh token** that you created in your Confluence account.

    > **Note**
    >
    > Select **Rotate secret** if you want Amazon Q to rotate the secret automatically so that you don't have to manually update the secret every time before you sync.

    c. Choose **Save and add secret**.
11. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

For more information, see VPC.

12. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

13. In **Sync scope**, choose from the following options :

a. In **Sync scope**, for **sync contents**, choose to sync from the following entity types: **Pages**, **Page comments**, **Page attachments**, **Blogs**, **Blog comments**, **Blog attachments**, **Personal spaces Archived spaces**, and **Archived pages**.

> **Note**
>
> **Page comments** and **Page attachments** can only be selected if you choose to sync **Pages**. **Blog comments** and **Blog attachments** can only be selected if you choose to sync **Blogs**.

> **Important**
>
> You can crawl **Pages** and **Blogs** from one of more specific **Spaces**. If you don't specify a **Space key** regex pattern in **Additional configuration**, all **Pages** and **Blogs** will be crawled by default. If no **Space** is specified in the filter, all spaces will be crawled.

b. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

To extract audio transcriptions and video content, enable processing for the following file types:

c. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

d. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

e. In **Additional configuration – *optional***, for **Space and regex patterns**, specify whether to include or exclude specific spaces, URLs, or file types in your index using the following:

- **Space key** – For example, `my-space-123`. Select **Add** after entering each space key you want to add.

> **Note**
>
> If you don't specify a **Space key** regex pattern in **Additional configuration**, all **Pages** and **Blogs** will be crawled by default. If no **Space** is specified in the filter, all spaces will be crawled.

- **URL** – For example, `.*/MySite/MyDocuments/`. Select **Add** after entering each URL you want to add.
- **File type** – For example, `.*\.pdf` or `.*\.txt`. Select **Add** after entering each file type you want to add.

- For **Entity title regex patterns** – Specify regular expression patterns to include or exclude certain **Blogs**, **Pages**, **Comments**, and **Attachments** by titles.

> **Note**
>
> If you want to crawl a specific page or subpage, you can use page title regex patterns to either include or exclude this page. Any valid regex pattern is supported. For example, if you use the regex `^QBusiness*`, any content starting with the word `QBusiness` followed by any number of characters will be filtered (`QBusiness_doc1` or `QBusiness`, but not `doc1_QBusiness`).

14. For **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

15. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.

16. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.

17. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

18. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Confluence (Cloud) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- Confluence configuration properties
- Confluence (Cloud) JSON schema

- Confluence (Cloud) JSON schema example

Confluence configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	This is the endpoint information for the data source. This is a sub-property for the `connectionConfiguration` .	`object` This property has the following sub-properties. • `hostUrl` • `type` • `authType`	Yes
`hostUrl`	The URL for your Confluence instance. For example, *`https://example.confluence.com`* .	`string` Specify the URL in the pattern `https://*`	Yes
`type`	The hosting method for your Confluence instance.	`string`	Yes

Configuration	Description	Type	Required
		The allowed values are SAAS or ON_PREM.	
authType	The authentication method for your Confluence instance.	string The allowed values are Basic or OAuth2.	Yes
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	object This property has the following sub-properties. • space • page • blog • comment • attachment	Yes

Configuration	Description	Type	Required
• space • page • blog • comment • attachment	A list of objects that map the attributes or field names of your Confluence spaces, pages, blogs, comments, and attachments to Amazon Q index field names.	object These properties have the following sub-properties. • indexFieldName • indexFieldType • dataSourceFieldName • dateFieldFormat	No
indexFieldName	The field name of your Confluence spaces, pages, blogs, comments, or attachments.	string	Yes
indexFieldType	The field type of your Confluence spaces, pages, blogs, comments, or attachments.	string The allowed values are STRING, STRING_LIST , and DATE.	Yes
dataSourceFieldName	The data source field name of your Confluence spaces, pages, blogs, comments, or attachments.	string	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The date format of your Confluenc e spaces, pages, blogs, comments, or attachments.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties. • isCrawlAcl • isRotateSecret • isCrawlPersonalSpace • isCrawlArchivedSpace • isCrawlArchivedPage • isCrawlPage • isCrawlBlog • isCrawlPageComment • isCrawlPageAttachment • isCrawlBlogComment • isCrawlBlogAttachment • fieldForUserId • maxFileSizeInMegaBytes	Yes

Configuration	Description	Type	Required
		• inclusionSpaceKeyFilter • exclusionSpaceKeyFilter • pageTitleRegEX • blogTitleRegEX • commentTitleRegEX • attachmentTitleRegEX • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionUrlPatterns • exclusionUrlPatterns	
isCrawlAcl	Specify true to crawl access control information from documents.	boolean	No
isRotateSecret	Specify true if you want to automatically rotate the secret.	boolean	No

Configuration	Description	Type	Required
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No
`proxyHost`	The host where the web proxy is required. The host name should be without protocol (http:// or https://).	`string`	Yes
`proxyPort`	Port used by the host URL transport protocol. The port number should be a numeric value between 0 and 65535.	`string`	Yes
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string` The allowed values are numbers between greater than 0 and less than or equal to 50.	No

Configuration	Description	Type	Required
• `inclusionSpaceKeyFilter` • `exclusionSpaceKeyFilter` • `pageTitleRegEX` • `blogTitleRegEX` • `commentTitleRegEX` • `attachmentTitleRegEX` • `inclusionFileTypePatterns` • `exclusionFileTypePatterns` • `inclusionUrlPatterns` • `exclusionUrlPatterns`	A list of regular expression patterns to include and/or exclude certain files in your Confluence data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.	`array (string)`	No

Configuration	Description	Type	Required
• isCrawlPersonalSpace • isCrawlArchivedSpace • isCrawlArchivedPage • isCrawlPage • isCrawlBlog • isCrawlPageComment • isCrawlPageAttachment • isCrawlBlogComment • isCrawlBlogAttachment	Specify true to index files in your Confluence personal spaces, pages, blogs, page comments, page attachments, blog comments, and blog attachments.	boolean	No
type	The type of data source. We recommend that you use CONFLUENCEV2 as your data source type.	string Valid values are CONFLUENCEV2 and CONFLUENCE .	Yes
enableIdentityCrawler	Specify true to activate identity crawler. Identity crawler is activated by default. See Identity crawler for more information.	boolean	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string Valid values are FORCED_FULL_CRAWL and FULL_CRAWL. You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index	Yes

Configuration	Description	Type	Required

`secretARN`	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains the key-value pairs required to connect to your Confluence instance.	`string`
		
		The minimum length is 20 and the maximum length is 2,048 characters.
		If you use basic authentication, the secret must contain a JSON structure with the following keys:
		
		`{ "username": " Confluence account user name", "password": "Confluence API token" }`
		
		If you use OAuth 2.0 authentication, the secret must contain a JSON structure with the following keys:
		
		`{ "confluenceAppKey": "app key for your Confluence account", "confluenceAppSecret": "app secret from`
			Yes

Configuration	Description	Type	Required
		your Confluence token", "confluenceAccessToken": "access token created in Confluence ", "confluenceRefreshToken": " refresh token created in Confluence " }	
version	The version of this template that's currently supported.	string	No

Confluence (Cloud) JSON schema

The following is the Confluence (Cloud) JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["CONFLUENCEV2", "CONFLUENCE"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
```

```
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "hostUrl": {
              "type": "string",
              "pattern": "https:.*"
            },
            "type": {
              "type": "string",
              "enum": ["SAAS"]
            },
            "authType": {
              "type": "string",
              "enum": ["Basic", "OAuth2"]
            }
          },
          "required": ["hostUrl", "type", "authType"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "space": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
```

```
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "page": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
```

```
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "blog": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
```

```
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "comment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
```

```
        "attachment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        }
      }
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "isCrawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
```

```
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "fieldForUserId": {
          "type": "string"
        },
        "inclusionSpaceKeyFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionSpaceKeyFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "pageTitleRegEX": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "blogTitleRegEX": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "commentTitleRegEX": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "attachmentTitleRegEX": {
          "type": "array",
          "items": {
            "type": "string"
```

```
          }
        },
        "isCrawlPersonalSpace": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlArchivedSpace": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlArchivedPage": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlPage": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
```

```
          ]
        },
        "isCrawlBlog": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlPageComment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlPageAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlBlogComment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
```

```
          ]
        },
        "isCrawlBlogAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionUrlPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionUrlPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "proxyHost": {
          "type": "string"
        },
        "proxyPort": {
```

```
          "type": "string"
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "type",
    "syncMode",
    "secretArn",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

Confluence (Cloud) JSON schema example

The following is the Confluence (Cloud) JSON schema example:

```
{
  "type": "CONFLUENCEV2",
  "syncMode": "FULL_CRAWL",
  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-confluence-
secret",
  "enableIdentityCrawler": "true",
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "hostUrl": "https://mycompany.atlassian.net",
      "type": "SAAS",
      "authType": "OAuth2"
    }
  },
  "repositoryConfigurations": {
    "space": {
      "fieldMappings": [
        {
          "indexFieldName": "space_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "page": {
      "fieldMappings": [
        {
          "indexFieldName": "page_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "blog": {
      "fieldMappings": [
        {
          "indexFieldName": "blog_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
```

```
    },
    "comment": {
      "fieldMappings": [
        {
          "indexFieldName": "comment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "attachment": {
      "fieldMappings": [
        {
          "indexFieldName": "attachment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    }
  },
  "additionalProperties": {
    "isCrawlAcl": "true",
    "fieldForUserId": "user_id",
    "inclusionSpaceKeyFilter": ["SPACE1", "SPACE2"],
    "exclusionSpaceKeyFilter": ["SPACE3"],
    "pageTitleRegEX": ["^.*$"],
    "blogTitleRegEX": ["^.*$"],
    "commentTitleRegEX": ["^.*$"],
    "attachmentTitleRegEX": ["^.*$"],
    "isCrawlPersonalSpace": "false",
    "isCrawlArchivedSpace": "false",
    "isCrawlArchivedPage": "true",
    "isCrawlPage": "true",
    "isCrawlBlog": "true",
    "isCrawlPageComment": "false",
    "isCrawlPageAttachment": "false",
    "isCrawlBlogComment": "true",
    "isCrawlBlogAttachment": "true",
    "maxFileSizeInMegaBytes": "50",
    "inclusionFileTypePatterns": ["*.pdf", "*.docx"],
    "exclusionFileTypePatterns": ["*.tmp"],
    "inclusionUrlPatterns": ["*"],
```

```
    "exclusionUrlPatterns": ["*.tmp"],
    "enableDeletionProtection": "false",
    "deletionProtectionThreshold": "15"
  }
}
```

Connecting Amazon Q Business to Confluence (Cloud) using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- Confluence configuration properties
- Confluence (Cloud) JSON schema for using the configuration property with AWS CloudFormation
- Confluence (Cloud) YAML schema for using the configuration property with AWS CloudFormation

Confluence configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes

Configuration	Description	Type	Required
`repositoryEndpointMetadata`	This is the endpoint information for the data source. This is a sub-property for the `connectionConfiguration` .	`object` This property has the following sub-properties. • `hostUrl` • `type` • `authType`	Yes
`hostUrl`	The URL for your Confluence instance. For example, *`https://example.confluence.com`* .	`string` Specify the URL in the pattern `https://*`	Yes
`type`	The hosting method for your Confluence instance.	`string` The allowed values are SAAS or `ON_PREM`.	Yes
`authType`	The authentication method for your Confluence instance.	`string` The allowed values are `Basic` or `OAuth2`.	Yes

Configuration	Description	Type	Required
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties. • `space` • `page` • `blog` • `comment` • `attachment`	Yes
• `space` • `page` • `blog` • `comment` • `attachment`	A list of objects that map the attributes or field names of your Confluence spaces, pages, blogs, comments, and attachments to Amazon Q index field names.	`object` These properties have the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName` • `dateFieldFormat`	No
`indexFieldName`	The field name of your Confluence spaces, pages, blogs, comments, or attachments.	`string`	Yes

Configuration	Description	Type	Required
`indexFieldType`	The field type of your Confluence spaces, pages, blogs, comments, or attachments.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes
`dataSourceFieldName`	The data source field name of your Confluence spaces, pages, blogs, comments, or attachments.	`string`	Yes
`dateFieldFormat`	The date format of your Confluence spaces, pages, blogs, comments, or attachments.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties. • isCrawlAcl • isRotateSecret • isCrawlPersonalSpace • isCrawlArchivedSpace • isCrawlArchivedPage • isCrawlPage • isCrawlBlog • isCrawlPageComment • isCrawlPageAttachment • isCrawlBlogComment • isCrawlBlogAttachment • fieldForUserId • maxFileSizeInMegaBytes	Yes

Configuration	Description	Type	Required
		• inclusionSpaceKeyFilter • exclusionSpaceKeyFilter • pageTitleRegEX • blogTitleRegEX • commentTitleRegEX • attachmentTitleRegEX • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionUrlPatterns • exclusionUrlPatterns	
isCrawlAcl	Specify true to crawl access control information from documents.	boolean	No
isRotateSecret	Specify true if you want to automatically rotate the secret.	boolean	No

Configuration	Description	Type	Required
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No
`proxyHost`	The host where the web proxy is required. The host name should be without protocol (http:// or https://).	`string`	Yes
`proxyPort`	Port used by the host URL transport protocol. The port number should be a numeric value between 0 and 65535.	`string`	Yes
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string` The allowed values are numbers between greater than 0 and less than or equal to 50.	No

Configuration	Description	Type	Required
• `inclusionSpaceKeyFilter` • `exclusionSpaceKeyFilter` • `pageTitleRegEX` • `blogTitleRegEX` • `commentTitleRegEX` • `attachmentTitleRegEX` • `inclusionFileTypePatterns` • `exclusionFileTypePatterns` • `inclusionUrlPatterns` • `exclusionUrlPatterns`	A list of regular expression patterns to include and/or exclude certain files in your Confluence data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.	`array (string)`	No

Configuration	Description	Type	Required
• isCrawlPersonalSpace • isCrawlArchivedSpace • isCrawlArchivedPage • isCrawlPage • isCrawlBlog • isCrawlPageComment • isCrawlPageAttachment • isCrawlBlogComment • isCrawlBlogAttachment	Specify true to index files in your Confluence personal spaces, pages, blogs, page comments, page attachments, blog comments, and blog attachments.	boolean	No
type	The type of data source. We recommend that you use CONFLUENCEV2 as your data source type.	string Valid values are CONFLUENCEV2 and CONFLUENCE .	Yes
enableIdentityCrawler	Specify true to activate identity crawler. Identity crawler is activated by default. See Identity crawler for more information.	boolean	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string Valid values are FORCED_FULL_CRAWL and FULL_CRAWL. You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index	Yes

Configuration	Description	Type	Required

`secretARN`	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains the key-value pairs required to connect to your Confluence instance.	`string`
		
		The minimum length is 20 and the maximum length is 2,048 characters.
		If you use basic authentication, the secret must contain a JSON structure with the following keys:
		
		`{ "username": " Confluence account user name", "password": "Confluence API token" }`
		
		If you use OAuth 2.0 authentication, the secret must contain a JSON structure with the following keys:
		
		`{ "confluenceAppKey": "app key for your Confluence account", "confluenceAppSecret": "app secret from`
			Yes

Configuration	Description	Type	Required
		your Confluence token", "confluenceAccessToken": "access token created in Confluence ", "confluenceRefreshToken": " refresh token created in Confluence " }	
version	The version of this template that's currently supported.	string	No

Confluence (Cloud) JSON schema for using the configuration property with AWS CloudFormation

The following is the Confluence (Cloud) JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- Confluence (Cloud) JSON schema for using the configuration property with AWS CloudFormation
- Confluence (Cloud) JSON schema example for using the configuration property with AWS CloudFormation

Confluence (Cloud) JSON schema for using the configuration property with AWS CloudFormation

The following is the Confluence (Cloud) JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
```

```
  "properties": {
    "type": {
      "type": "string",
      "enum": ["CONFLUENCEV2", "CONFLUENCE"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "hostUrl": {
              "type": "string",
              "pattern": "https:.*"
            },
            "type": {
              "type": "string",
              "enum": ["SAAS"]
            },
            "authType": {
              "type": "string",
              "enum": ["Basic", "OAuth2"]
            }
          },
```

```
          "required": ["hostUrl", "type", "authType"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "space": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "page": {
```

```
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "blog": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "comment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
```

```
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "attachment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
```

```
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "isCrawlAcl": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "fieldForUserId": {
        "type": "string"
      },
      "inclusionSpaceKeyFilter": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionSpaceKeyFilter": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "pageTitleRegEX": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
```

```
        "blogTitleRegEX": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "commentTitleRegEX": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "attachmentTitleRegEX": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "isCrawlPersonalSpace": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlArchivedSpace": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlArchivedPage": {
          "anyOf": [
            {
              "type": "boolean"
```

```
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlPage": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlBlog": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlPageComment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlPageAttachment": {
          "anyOf": [
            {
              "type": "boolean"
```

```
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlBlogComment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlBlogAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
```

```
        "inclusionUrlPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionUrlPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "proxyHost": {
          "type": "string"
        },
        "proxyPort": {
          "type": "string"
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
```

```
    ]
  },
  "required": [
    "type",
    "syncMode",
    "secretArn",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

Confluence (Cloud) JSON schema example for using the configuration property with AWS CloudFormation

The following is the Confluence (Cloud) JSON schema example for the configuration property for CloudFormation

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation CONFLUENCE Data Source Template",
  "Resources": {
    "DataSourceConfluence": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MyConfluenceDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "CONFLUENCEV2",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-
confluence-secret",
          "enableIdentityCrawler": "true",
          "connectionConfiguration": {
            "repositoryEndpointMetadata": {
              "hostUrl": "https://mycompany.atlassian.net",
              "type": "SAAS",
              "authType": "OAuth2"
            }
          },
          "repositoryConfigurations": {
```

```
            "space": {
              "fieldMappings": [
                {
                  "indexFieldName": "space_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
            },
            "page": {
              "fieldMappings": [
                {
                  "indexFieldName": "page_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
            },
            "blog": {
              "fieldMappings": [
                {
                  "indexFieldName": "blog_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
            },
            "comment": {
              "fieldMappings": [
                {
                  "indexFieldName": "comment_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
            },
            "attachment": {
              "fieldMappings": [
                {
                  "indexFieldName": "attachment_id",
```

```
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          }
        },
        "additionalProperties": {
          "isCrawlAcl": "true",
          "fieldForUserId": "user_id",
          "inclusionSpaceKeyFilter": ["SPACE1", "SPACE2"],
          "exclusionSpaceKeyFilter": ["SPACE3"],
          "pageTitleRegEX": ["^.*$"],
          "blogTitleRegEX": ["^.*$"],
          "commentTitleRegEX": ["^.*$"],
          "attachmentTitleRegEX": ["^.*$"],
          "isCrawlPersonalSpace": "false",
          "isCrawlArchivedSpace": "false",
          "isCrawlArchivedPage": "true",
          "isCrawlPage": "true",
          "isCrawlBlog": "true",
          "isCrawlPageComment": "false",
          "isCrawlPageAttachment": "false",
          "isCrawlBlogComment": "true",
          "isCrawlBlogAttachment": "true",
          "maxFileSizeInMegaBytes": "50",
          "inclusionFileTypePatterns": ["*.pdf", "*.docx"],
          "exclusionFileTypePatterns": ["*.tmp"],
          "inclusionUrlPatterns": ["*"],
          "exclusionUrlPatterns": ["*.tmp"],
          "enableDeletionProtection": "false",
          "deletionProtectionThreshold": "15"
        }
      }
    }
  }
}
```

Confluence (Cloud) YAML schema for using the configuration property with AWS CloudFormation

The following is the Confluence (Cloud) YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- Confluence (Cloud) YAML schema for using the configuration property with AWS CloudFormation
- Confluence (Cloud) YAML schema example for using the configuration property with AWS CloudFormation

Confluence (Cloud) YAML schema for using the configuration property with AWS CloudFormation

The following is the Confluence (Cloud) YAML schema for the configuration property for CloudFormation.

```
type: object
properties:
  type:
    type: string
    enum:
      - CONFLUENCEV2
      - CONFLUENCE
  syncMode:
    type: string
    enum:
      - FULL_CRAWL
      - FORCED_FULL_CRAWL
  secretArn:
    type: string
    minLength: 20
    maxLength: 2048
  enableIdentityCrawler:
    anyOf:
      - type: boolean
      - type: string
        enum:
          - "true"
          - "false"
  connectionConfiguration:
```

```
    type: object
    properties:
      repositoryEndpointMetadata:
        type: object
        properties:
          hostUrl:
            type: string
            pattern: "https:.*"
          type:
            type: string
            enum:
              - SAAS
          authType:
            type: string
            enum:
              - Basic
              - OAuth2
        required:
          - hostUrl
          - type
          - authType
    required:
      - repositoryEndpointMetadata
  repositoryConfigurations:
    type: object
    properties:
      space:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
```

```
            dateFieldFormat:
              type: string
              pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
      required:
        - fieldMappings
    page:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
                  - LONG
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
      required:
        - fieldMappings
    blog:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
```

```
                - DATE
                - LONG
            dataSourceFieldName:
              type: string
            dateFieldFormat:
              type: string
              pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
      required:
        - fieldMappings
    comment:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
                  - LONG
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
      required:
        - fieldMappings
    attachment:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
```

```
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
                  - LONG
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
      required:
        - fieldMappings
additionalProperties:
  type: object
  properties:
    isCrawlAcl:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    fieldForUserId:
      type: string
    inclusionSpaceKeyFilter:
      type: array
      items:
        type: string
    exclusionSpaceKeyFilter:
      type: array
      items:
        type: string
    pageTitleRegEX:
      type: array
      items:
        type: string
    blogTitleRegEX:
      type: array
      items:
        type: string
    commentTitleRegEX:
      type: array
      items:
```

```
        type: string
    attachmentTitleRegEX:
      type: array
      items:
        type: string
    isCrawlPersonalSpace:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    isCrawlArchivedSpace:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    isCrawlArchivedPage:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    isCrawlPage:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    isCrawlBlog:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    isCrawlPageComment:
      anyOf:
        - type: boolean
        - type: string
```

```
        enum:
          - "true"
          - "false"
    isCrawlPageAttachment:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    isCrawlBlogComment:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    isCrawlBlogAttachment:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    maxFileSizeInMegaBytes:
      type: string
    inclusionFileTypePatterns:
      type: array
      items:
        type: string
    exclusionFileTypePatterns:
      type: array
      items:
        type: string
    inclusionUrlPatterns:
      type: array
      items:
        type: string
    exclusionUrlPatterns:
      type: array
      items:
        type: string
    proxyHost:
      type: string
```

```
      proxyPort:
        type: string
      enableDeletionProtection:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
        default: false
      deletionProtectionThreshold:
        type: string
        default: "15"
    required: []
version:
  type: string
  anyOf:
    - pattern: 1.0.0
required:
  - type
  - syncMode
  - secretArn
  - connectionConfiguration
  - repositoryConfigurations
  - additionalProperties
```

Confluence (Cloud) YAML schema example for using the configuration property with AWS CloudFormation

The following is the Confluence (Cloud) YAML example for the Configuration property for CloudFormation:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: CloudFormation CONFLUENCE Data Source Template
Resources:
  DataSourceConfluence:
    Type: AWS::QBusiness::DataSource
    Properties:
      ApplicationId: app12345-1234-1234-1234-123456789012
      IndexId: indx1234-1234-1234-1234-123456789012
      DisplayName: MyConfluenceDataSource
      RoleArn: arn:aws:iam::123456789012:role/qbusiness-data-source-role
      Configuration:
```

```
        type: CONFLUENCEV2
        syncMode: FULL_CRAWL
        secretArn: arn:aws:secretsmanager:us-west-2:123456789012:secret:my-confluence-
secret
        enableIdentityCrawler: "true"
        connectionConfiguration:
          repositoryEndpointMetadata:
            hostUrl: https://mycompany.atlassian.net
            type: SAAS
            authType: OAuth2
        repositoryConfigurations:
          space:
            fieldMappings:
              - indexFieldName: space_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
          page:
            fieldMappings:
              - indexFieldName: page_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
          blog:
            fieldMappings:
              - indexFieldName: blog_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
          comment:
            fieldMappings:
              - indexFieldName: comment_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
          attachment:
            fieldMappings:
              - indexFieldName: attachment_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
        additionalProperties:
          isCrawlAcl: "true"
          fieldForUserId: user_id
```

```
          inclusionSpaceKeyFilter:
            - SPACE1
            - SPACE2
          exclusionSpaceKeyFilter:
            - SPACE3
          pageTitleRegEX:
            - "^.*$"
          blogTitleRegEX:
            - "^.*$"
          commentTitleRegEX:
            - "^.*$"
          attachmentTitleRegEX:
            - "^.*$"
          isCrawlPersonalSpace: "false"
          isCrawlArchivedSpace: "false"
          isCrawlArchivedPage: "true"
          isCrawlPage: "true"
          isCrawlBlog: "true"
          isCrawlPageComment: "false"
          isCrawlPageAttachment: "false"
          isCrawlBlogComment: "true"
          isCrawlBlogAttachment: "true"
          maxFileSizeInMegaBytes: "50"
          inclusionFileTypePatterns:
            - "*.pdf"
            - "*.docx"
          exclusionFileTypePatterns:
            - "*.tmp"
          inclusionUrlPatterns:
            - "*"
          exclusionUrlPatterns:
            - "*.tmp"
          enableDeletionProtection: "false"
          deletionProtectionThreshold: "15"
```

How Amazon Q Business connector crawls Confluence (Cloud) ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect a Confluence (Cloud) data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your Confluence (Cloud) instance. If you choose to activate ACL crawling, the information can be used to filter chat responses based your end users' document access level.

The connector crawls the following Confluence resources:

- **Spaces** – A collection of related pages, blogs, and attachments. Space permissions apply to all documents in the space by default.
- **Pages** – Documents in a space where users create and manage content. Pages can contain text, images, tables, and multimedia elements, and can have nested pages. Each page is considered a single document. Pages can be restricted to specific users and groups in the space. A nested page inherits restrictions from the parent page, and can have its own restrictions.
- **Blogs** – Content similar to pages, typically used for updates or announcements. Each blog post is considered as a single document. Blogs can be restricted to specific users and groups in the space.
- **Comments** – Feedback and discussions on pages or blog post content. Comments are visible to viewers of the page or post.
- **Attachments** – Files uploaded to pages or blog posts, such as images and documents.

The connector also crawls user principal information (local user alias, local group and federated group identity configurations) and its permissions for each configured space. The Confluence (Cloud) connector does not support crawling macros, whiteboards, or databases.

The connector updates ACL changes each time it crawls your data source content. To ensure that the correct users have access to the correct content, regularly re-sync your data source to capture any ACL updates.

You configure user and group access to spaces using the space permissions page. For pages and blogs, you use the restrictions page. For more information about space permissions, see Space Permissions Overview on the Confluence Support website. For more information about page and blog restrictions, see Page Restrictions on the Confluence Support website.

> **Important**
>
> For user context filtering to work correctly, users' visibility must be set to **Anyone**. For more information, see Set your email visibility in Atlassian Developer Documentation.

The group and user IDs are mapped as follows:

- `_group_ids` – Group names are present on spaces, pages, and blogs where there are restrictions. They're mapped from the name of the group in Confluence . Group names are always lower case.
- `_user_id` – User names are present on the space, page, or blog where there are restrictions. They're mapped depending on the type of Confluence instance that you are using.

For Confluence (Cloud) – The `_user_id` is the account ID of the user.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Amazon Q Business Confluence (Cloud) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application environment and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Confluence connector supports the following entities and the associated reserved and custom attributes.

> **Important**
>
> If you map any Confluence (Cloud) field to Amazon Q document title and document body fields, Amazon Q will generate responses from data in the document title and body.

Supported entities and field mappings

- Space
- Page
- Blog
- Comment
- Attachment

Space

Confluence field name	Index field name	Description	Data type
spaceName	cf_sp_document_title	Custom	String
itemType	_category	Default	String
url	_source_uri	Default	String
spaceKey	cf_space_key	Custom	String

Confluence field name	Index field name	Description	Data type
description	cf_description	Custom	String
spaceType	cf_type	Custom	String

Page

Confluence field name	Index field name	Description	Data type
title	_cf_page_document_title	Custom	String
authors	_authors	Default	String list
createdDate	_created_at	Default	Date
modifiedDate	_last_updated_at	Default	Date
labels	cf_labels	Custom	String list
version	cf_version	Custom	Long (numeric)
itemType	_category	Default	String
spaceKey	cf_space_key	Custom	String
spaceName	cf_space_name	Custom	String
url	_source_uri	Default	String
status	cf_status	Custom	String
parentId	cf_parent_id	Custom	String

Blog

Confluence field name	Index field name	Description	Data type
title	cf_bg_document_title	Custom	String
author	_authors	Default	String list
publishedDate	_created_at	Default	Date
labels	_source_uri	Default	String
version	cf_version	Custom	Long (numeric)
itemType	_category	Custom	String
spaceKey	cf_space_key	Custom	String
modifiedDate	_last_updated_at	Default	Date
spaceName	cf_space_name	Custom	String
status	cf_status	Custom	String
url	_source_uri	Default	String
parentId	cf_parent_id	Custom	String

Comment

Confluence field name	Index field name	Description	Data type
title	cf_cmt_document_title	Custom	String
author	_authors	Default	String list
createdDate	_created_at	Default	Date

Confluence field name	Index field name	Description	Data type
version	cf_version	Custom	Long (numeric)
itemType	_category	Default	String
spaceKey	cf_space_key	Custom	String
spaceName	cf_space_name	Custom	String
contentType	cf_content_type	Custom	String
url	_source_uri	Default	String
parentId	cf_parent_id	Custom	String
status	cf_status	Custom	String

Attachment

Confluence field name	Index field name	Description	Data type
fileName	cf_attachment_document_title	Custom	String
author	_authors	Default	String list
createdDate	_created_at	Default	Date
labels	cf_labels	Custom	String list
version	cf_version	Custom	Long (numeric)
itemType	_category	Default	String
spaceKey	cf_space_key	Custom	String
contentType	cf_content_type	Custom	String

Confluence field name	Index field name	Description	Data type
modifiedDate	_last_updated_at	Default	Date
fileSize	cf_file_size	Custom	Long (numeric)
fileType	cf_attachment_file_type	Custom	String
spaceName	cf_space_name	Custom	String
documentId	_document_id	Default	String list
url	_source_uri	Default	String
parentId	cf_parent_id	Custom	String
attachmentComment	cf_attachment_comment	Custom	String
status	cf_status	Custom	String

IAM role for Amazon Q Confluence (Cloud) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.

- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
```

```
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
```

```
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the Amazon Q Business Confluence (Cloud) connector

The following table provides information about error codes you may see for the Confluence (Cloud) connector and suggested resolutions.

Error code	Error message	Suggested resolution
CNF-5500	Null/empty username.	Provide username.
CNF-5501	Error validating credentials due to Invalid username or password.	Provide valid username/password
CNF-5502	Null/empty confluence AppKey.	Provide confluence AppKey.
CNF-5503	Null/empty confluence Secret.	Provide confluence Secret.
CNF-5504	Null/empty Client Access Token.	Provide Client Access Token.
CNF-5505	Null/empty Client Refresh Token	Provide Client Refresh Token
CNF-5506	Incorrect auth type.	Auth type should be Basic or OAuth2 or Personal-token.
CNF-5507	Null/empty auth type.	Auth Type should not be null or empty value.
CNF-5508	Empty/null host URL.	Host Url should not be null or empty value.
CNF-5509	Null/empty crawl type.	Crawl Type should not be null or empty value.
CNF-5510	Null/empty Repository Configurations.	Repository Configurations should not be null or empty value.

Error code	Error message	Suggested resolution
CNF-5511	Incorrect type.	type should be SAAS or ON_PREM.
CNF-5512	Invalid inclusion file type patterns.	Provide the correct inclusion patterns.
CNF-5513	Invalid exclusion file type patterns.	Provide the correct exclusion patterns.
CNF-5514	Invalid regex patterns.	Provide the correct regex patterns.
CNF-5515	Error validating credentials due to invalid username or password.	Provide valid username and password.
CNF-5516	Error validating credentials due to invalid client id or client secret.	Provide valid client id and client secret.
CNF-5517	Error validating crawl type.	Provide valid crawl type.
CNF-5518	Invalid URI.	Provide valid URI.
CNF-5519	Null/empty DataSourceFieldName in Space Entity.	Provide value for DataSourceFieldName in Space Entity.
CNF-5520	Null/empty IndexFieldName in Blog Entity.	Provide value for IndexFieldName in Blog Entity.
CNF-5521	Null/empty IndexFieldType in Space Entity.	Provide value for IndexFieldType in Space Entity.
CNF-5522	Null/empty password.	Provide password.
CNF-5523	Incorrect auth type.	Auth type should be Basic or OAuth2.

Error code	Error message	Suggested resolution
CNF-5524	Null/empty DataSourceFieldName in Page Entity.	Provide value for DataSourceFieldName in Page Entity.
CNF-5525	Null/empty DataSourceFieldName in Blog Entity	Please provide value for DataSourceFieldName in Blog Entity
CNF-5526	Null/empty DataSourceFieldName in Comment Entity.	Provide value for DataSourceFieldName in Comment Entity.
CNF-5527	Null/empty DataSourceFieldName in Attachment Entity.	Provide value for DataSourceFieldName in Attachment Entity.
CNF-5528	Null/empty IndexFieldName.	IndexFieldName field can't be null or empty value.
CNF-5529	Null/empty IndexFieldName in Space Entity.	Provide value for IndexFieldName in Space Entity.
CNF-5530	Null/empty IndexFieldName in Page Entity	Please provide value for IndexFieldName in Page Entity
CNF-5531	Invalid isCrawlPersonalSpace value.	isCrawlPersonalSpace should be a boolean value true or false.
CNF-5532	Invalid isCrawlArchivedSpace value.	isCrawlArchivedSpace should be a boolean value true or false.
CNF-5533	Invalid isCrawlArchivedPage value.	isCrawlArchivedPage should be a boolean value true or false.
CNF-5534	Invalid isCrawlPage value.	isCrawlPage should be a boolean value true or false.

Error code	Error message	Suggested resolution
CNF-5535	Invalid isCrawlBl ogComment value.	isCrawlBlogComment should be a boolean value true or false.
CNF-5536	Invalid isCrawlBl ogComment value.	isCrawlBlogComment should be a boolean value true or false.
CNF-5537	Invalid isCrawlBl ogAttachment value.	isCrawlBlogAttachment should be a boolean value true or false.
CNF-5538	Error validating on protocol.	Provide valid protocol.
CNF-5539	Null/empty IndexFiel dName in Comment Entity.	Provide value for IndexFieldName in Comment Entity.
CNF-5540	Null/empty Personal Access Token.	Provide Personal Access Token.
CNF-5541	Invalid OAuth value.	Give a valid OAuth URL.
CNF-5542	Invalid Space value.	Give a valid Space URL.
CNF-5543	Archived Space Exception .	Check Archived Space.
CNF-5544	JSON Exception for Space.	Check Space.
CNF-5545	JSON Exception for Comment.	Check Comment.
CNF-5546	JSON Exception for Comment.	Check Comment.
CNF-5547	JSON Exception for Comment.	Check Comment.

Error code	Error message	Suggested resolution
CNF-5548	JSON Exception for Attachment.	Check Attachment.
CNF-5549	JSON Exception for Blog.	Check Blog.
CNF-5550	JSON Exception for Page.	Check Page.
CNF-5551	JSON Exception for Label.	Check Label.
CNF-5552	JSON Exception for ACL.	Check ACL.
CNF-5553	JSON Exception for Groups.	Check Groups.
CNF-5554	JSON Exception for Group Members.	Check Group Members.
CNF-5555	JSON Exception for Space Group.	Check Space Group.
CNF-5556	Exception in CommentIt em.	Check the CommentItem class.
CNF-5557	Invalid isCrawlPa geComment value.	isCrawlPageComment should be a boolean value true or false.
CNF-5558	Invalid isCrawlPa geAttachment value.	isCrawlPageAttachment should be a boolean value true or false.
CNF-5559	Null/empty Repository Configurations.	Repository Configurations should not be null or empty value.
CNF-5560	Null/empty IndexFiel dName in Attachment.	Please provide value for IndexFiel dName in Attachment Entity.
CNF-5561	Invalid proxy url.	Proxy url should not contain http: or https.

Error code	Error message	Suggested resolution
CNF-5562	Null/Empty proxy port.	Provide a valid proxy port.
CNF-5563	Invalid Host URL.	Provide valid Host URL.
CNF-5564	Invalid proxy port value.	Provide a valid proxy port.
CNF-5565	Confluence server not reachable.	Provide a valid proxy and server details.
CNF-5566	Null/empty IndexFiel dType in Page Entity.	Provide value for IndexFieldType in Page Entity.
CNF-5567	Null/empty IndexFiel dType in Blog Entity.	Provide value for IndexFieldType in Blog Entity.
CNF-5568	Null/empty IndexFiel dType in Comment Entity.	Provide value for IndexFieldType in Comment Entity.
CNF-5569	Null/empty IndexFiel dType in Attachment.	Provide value for IndexFieldType in Attachment. Entity
CNF-5570	JSON Exception for Content Ancestors.	Check your Ancestors.
CNF-5571	Invalid Host URL Pattern.	Provide valid Host URL Pattern.
CNF-5572	Error validating credentia ls due to Invalid access or refresh token.	Invalid AccessToken/RefreshToken.

Connecting Confluence (Server/Data Center) to Amazon Q Business

Atlassian Confluence is a collaborative work-management tool designed for sharing, storing, and working on project planning, software development, and product management. You can connect Confluence (Server/Data Center) instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the Amazon Q Business Confluence (Server/Data Center) connector
- Confluence (Server/Data Center) connector overview
- Prerequisites for connecting Amazon Q to Confluence (Server/Data Center)
- Checking Confluence (Server/Data Center) connectivity
- Connecting Amazon Q Business to Confluence (Server/Data Center) using the console
- Connecting Amazon Q Business to Confluence (Server/Data Center) using APIs
- Connecting Amazon Q Business to Confluence (Server/Data Center) using AWS CloudFormation
- How Amazon Q Business connector crawls Confluence (Server/Data Center) ACLs
- Amazon Q Business Confluence (Server/Data Center) data source connector field mappings
- IAM role for Amazon Q Confluence (Server/Data Center) connector
- Understand error codes in the Amazon Q Business Confluence (Server/Data Center) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Amazon Q Business Confluence (Server/Data Center) connector

The Amazon Q Confluence (Server/Data Center) connector has the following known limitation:

- Because Amazon Q Business uses email addresses as unique identifiers, each user must have a unique email address.
- The Confluence (Server/Data Center) connector may not accurately differentiate between Confluence users with duplicate email addresses when mapping access control lists (ACLs). This can lead to inconsistent search results, in which a user might be able to see restricted content intended for one Confluence user with a shared email, but not other restricted content intended for a different Confluence user with the same email.

Confluence (Server/Data Center) connector overview

The following table gives an overview of the Amazon Q Business Confluence (Server/Data Center) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic, OAuth 2.0 with Refresh Token Flow, Personal Access Token
	Authentication credentials	For Basic authentication: • Confluence Server/Data Center username • Confluence Server/Data Center password For OAuth 2.0 authentication with Refresh Token Flow: • App key • App secret • Access token • Refresh token **Note** Access and refresh tokens expire in 1 hour. For information on regenerating tokens, see Atlassian Developer Documentation. Personal Access Token • Personal Access Token
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.

Category	Feature	Support
	Identity crawling	Yes
Crawl features	Custom metadata	Yes
	Entities	Yes. The following entities are supported: • Space • Page • Blog post • Comment • Attachment See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Inclusion exclusion filters for **Space key** and **Space URL** • Inclusion exclusion filters on **File Type** for **Attachment entity** • Supports regex filters for entities • Supports inclusion and exclusion filters for **File size**
	Sync mode	Supports full and incremental (new, modified, and deleted) sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q to Confluence (Server/Data Center)

Before you begin, make sure that you have completed the following prerequisites.

In Confluence Server/Data Center, make sure you have:

- Copied your Confluence instance URL. For example: *https://example.confluence.com*. You need your Confluence instance URL to connect to Amazon Q.
- Configured basic authentication credentials containing a username (username used to log into Confluence) and password (Confluence Server/Data Center password) to allow Amazon Q to connect to your Confluence Server/Data Center instance.
- **Optional:** Configured OAuth 2.0 credentials containing a Confluence app key, Confluence app secret, Confluence access token, and Confluence refresh token to allow Amazon Q to connect to your Confluence instance. If your access token expires, you can either use the refresh token to regenerate your access token and refresh token pair, or you can repeat the authorization process.
- **Optional:** Configured a Personal Access Token (PAT) containing a Confluence token to allow Amazon Q to connect to your Confluence Server/Data Center instance. For information about how to create a PAT token, see Using Personal Access Tokens on the Atlassian website.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- If you want to have Amazon Q automatically rotate your secret, ensure that your IAM role includes the `secretsmanager:PutSecretValue` and `secretsmanager:UpdateSecret` permissions.
- Stored your Confluence (Server/Data Center) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Checking Confluence (Server/Data Center) connectivity

Before you sync your Confluence (Server/Data Center) data source connector after configuring it, we recommend you check the connection between Amazon Q Business and Confluence (Server/Data Center). The following are the cURL commands you need to check Confluence (Server/Data Center) connectivity.

Topics

- Checking basic authentication connectivity
- Checking personal access token connectivity

Checking basic authentication connectivity

To check connectivity for a Confluence (Server/Data Center) data source connector using basic authentication, use the following cURL command:

```
curl --location 'https://<confluence_host-url>/wiki/rest/api/user/current'
--header 'Authorization: Basic <Base64 encoded username and password>'
```

If your data source is connected as expected, the JSON response should resemble the following:

```
{
    "type": "known",
    "accountId": "accountId",
    "accountType": "atlassian",
    "email": "email",
    "publicName": "Administrator",
    "profilePicture": {
        "path": "/wiki/aa-avatar/<accountId>",
        "width": 48,
        "height": 48,
        "isDefault": false
    },
    "displayName": "Administrator",
    "isExternalCollaborator": false,
    "_expandable": {
        "operations": "",
        "personalSpace": ""
    },
    "_links": {
```

```
        "self": "https://<host_url>/wiki/rest/api/user?accountId=<accountId>",
        "base": "https://<host_url>/wiki",
        "context": "/wiki"
    }
}
```

If your Confluence (Server/Data Center) connector is not connected correctly, you will see the following error:

- CNF-5123: The profile value is invalid. Try again after sometime.

To troubleshoot the issue, check your Confluence (Server/Data Center) URL and make sure it's correct.

Checking personal access token connectivity

To check connectivity for a Confluence (Server/Data Center) data source connector using personal access token authentication, use the following cURL command:

```
curl --location 'https://<confluence_server_host_url>/rest/api/user/current'
--header 'Authorization: Bearer <PAT_TOKEN>'
```

If your data source is connected as expected, the JSON response should resemble the following:

```
{
    "type": "known",
    "accountId": "accountId",
    "accountType": "atlassian",
    "email": "email",
    "publicName": "Administrator",
    "profilePicture": {
        "path": "/wiki/aa-avatar/<accountId>",
        "width": 48,
        "height": 48,
        "isDefault": false
    },
    "displayName": "Administrator",
    "isExternalCollaborator": false,
    "_expandable": {
        "operations": "",
        "personalSpace": ""
```

```
    },
    "_links": {
        "self": "https://<host_url>/wiki/rest/api/user?accountId=<accountId>",
        "base": "https://<host_url>/wiki",
        "context": "/wiki"
    }
}
```

If your Confluence (Server/Data Center) connector is not connected correctly, you will see the following error:

- CNF-5123: The profile value is invalid. Try again after sometime.

To troubleshoot the issue, check your Confluence (Server/Data Center) URL and make sure it's correct.

Connecting Amazon Q Business to Confluence (Server/Data Center) using the console

On the **Confluence** page, enter the following information:

1. **Name and description**, do the following:
   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
2. In **Source**, enter the following information:
   a. In **Source**, for **Hosting Method** – Choose **Confluence Server/Data Center**.
   b. **Confluence URL** – Enter the Confluence host URLs. The format for the host URL that you enter is *https://example.confluence.com*.

> **Important**
>
> If you change or update your Confluence (Server/Data Center) data source URL, you also need to update your Secrets Manager secret to ensure a secure connection.

c. **SSL certificate location** – Enter the file path to an SSL certificate stored in an Amazon S3 bucket.

3. **Web proxy – *optional***, enter the following information:

   a. **Host name** – Host name for your Confluence account.

   b. **Port number** – Port used by the host URL transport protocol.

4. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

5. For **Authentication** – Choose between **Basic authentication**, **Oauth 2.0 authentication**, and **Personal Access Token authentication** based on your use case.

6. **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your Confluence authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens. Enter the following information in the window:

   a. **Secret name** – A name for your secret.

   b. If using **Basic Authentication** – Enter the **Secret name Username**, and **Password** (Confluence Server/Data Center password) that you generated and downloaded from your Confluence account.

      If using **OAuth2.0 Authentication** – Enter the **Secret name**, **App key**, **App secret**, **Access token**, and **Refresh token** you created in your Confluence account.

      If using **Personal Access Token authentication** – Enter the **Secret name** and the **Confluence Server PAT token** that you created in your Confluence Server account.

> **Note**
>
> Select **Rotate secret** if you want Amazon Q to rotate the secret automatically so that you don't have to manually update the secret every time you sync.

c. Choose **Save and add secret**.

7. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

   a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

   b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

   For more information, see VPC.

8. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

   > **Note**
   >
   > Creating a new service IAM role is recommended.

   For more information, see IAM role.

9. In **Sync scope**, choose from the following options:

   a. In **Sync scope**, for **sync contents**, choose to sync from the following entity types: **Pages**, **Page comments**, **Page attachments**, **Blogs**, **Blog comments**, **Blog attachments**, **Personal spaces**, and **Archived spaces**.

> **Note**
>
> **Page comments** and **Page attachments** can only be selected if you choose to sync **Pages**. **Blog comments** and **Blog attachments** can only be selected if you choose to sync **Blogs**.

> **Important**
>
> You can crawl **Pages** and **Blogs** from one of more specific **Spaces**. If you don't specify a **Space key** regex pattern in **Additional configuration**, all **Pages** and **Blogs** will be crawled by default. If no **Space** is specified in the filter, all spaces will be crawled.

b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

c. In **Additional configuration – *optional***, for **Space and regex patterns**, specify whether to include or exclude specific spaces, URLs, or file types in your index using the following:

- **Space key** – For example, *`my-space-123`*. Select **Add** after entering each space key you want to add.

  > **Note**
  >
  > If you don't specify a **Space key** regex pattern in **Additional configuration**, all **Pages** and **Blogs** will be crawled by default. If no **Space** is specified in the filter, all spaces will be crawled.

- **URL** – For example, *`.*/MySite/MyDocuments/`*. Select **Add** after entering each URL you want to add.
- **File type** – For example, *`.*\.pdf`* or *`.*\.txt`*. Select **Add** after entering each file type you want to add.

- For **Entity title regex patterns** – Specify regular expression patterns to include or exclude certain **Blogs**, **Pages**, **Comments**, and **Attachments** by titles.

> **Note**
>
> If you want to crawl a specific page or subpage, you can use page title regex patterns to either include or exclude this page.

d. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

   To extract audio transcriptions and video content, enable processing for the following file types:

e. **Advanced settings**

   Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

10. For **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

11. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.

12. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.

13. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

14. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Confluence (Server/Data Center) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- Confluence (Server/Data Center) configuration properties
- Confluence (Server/Data Center) JSON schema
- Confluence (Server/Data Center) JSON schema example

Confluence (Server/Data Center) configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has the following sub-property: `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-properties: `hostUrl`, `type`, and `authType`.	Yes
`hostUrl`	The URL for your Confluence instance. For example, *`https://example.confluence.com`* .	`string` Specify the URL in the pattern `https://*`	Yes

Configuration	Description	Type	Required
	Important If you change or update your Confluence (Server/Data Center) data source URL, you also need to update your Secrets Manager secret to ensure a secure connection.		
`type`	The hosting method for your Confluence instance.	`string` The allowed values are SAAS or `ON_PREM`.	Yes
`authType`	The authentication method for your Confluence instance.	`string` The allowed values are `Basic`, `OAuth2`, or `Personal-token` .	Yes

Configuration	Description	Type	Required
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties: `space`, `page`, `blog`, `comment`, and `attachment` .	Yes
• `space` • `page` • `blog` • `comment` • `attachment`	A list of objects that map the attributes or field names of your Confluence spaces, pages, blogs, comments, and attachments to Amazon Q index field names.	`object` These properties have the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName` • `dateFieldFormat`	No
`indexFieldName`	The field name of your Confluence spaces, pages, blogs, comments, or attachments.	`string`	Yes
`indexFieldType`	The field type of your Confluence spaces, pages, blogs, comments, or attachments.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes

Configuration	Description	Type	Required
`dataSourceFieldName`	The data source field name of your Confluence spaces, pages, blogs, comments, or attachments.	`string`	Yes
`dateFieldFormat`	The date format of your Confluence spaces, pages, blogs, comments, or attachments.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties. • isCrawlAcl • isRotateSecret • isCrawlPersonalSpace • isCrawlArchivedSpace • isCrawlArchivedPage • isCrawlPage • isCrawlBlog • isCrawlPageComment • isCrawlPageAttachment • isCrawlBlogComment • isCrawlBlogAttachment • fieldForUserId • maxFileSizeInMegaBytes	Yes

Configuration	Description	Type	Required
		• inclusionSpaceKeyFilter • exclusionSpaceKeyFilter • pageTitleRegEX • blogTitleRegEX • commentTitleRegEX • attachmentTitleRegEX • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionUrlPatterns • exclusionUrlPatterns • proxyHost • proxyPort	

Configuration	Description	Type	Required
`isCrawlAcl`	Specify `true` to crawl access control information from documents. **Note** Amazon Q Business crawls ACL information to ensure responses are generated only from documents your end users have access to by default. See Authorization for more details.	`boolean`	No
`isRotateSecret`	Specify `true` if you want to automatically rotate the secret.	`boolean`	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No

Configuration	Description	Type	Required
`proxyHost`	The host where the web proxy is required. The host name should be without protocol (http:// or https://).	`string`	No
`proxyPort`	Port used by the host URL transport protocol. The port number should be a numeric value between 0 and 65535.	`string`	No
`maxFileSizeInMegaBytes`	Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string`	No

Configuration	Description	Type	Required
• inclusionSpaceKeyFilter • exclusionSpaceKeyFilter • pageTitleRegEX • blogTitleRegEX • commentTitleRegEX • attachmentTitleRegEX • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionUrlPatterns • exclusionUrlPatterns	A list of regular expression patterns to include and/or exclude certain files in your Confluence data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.	array (string)	No

Configuration	Description	Type	Required
• `isCrawlPersonalSpace` • `isCrawlArchivedSpace` • `isCrawlArchivedPage` • `isCrawlPage` • `isCrawlBlog` • `isCrawlPageComment` • `isCrawlPageAttachment` • `isCrawlBlogComment` • `isCrawlBlogAttachment`	`true` to index files in your Confluence personal spaces, pages, blogs, page comments, page attachments, blog comments, and blog attachments.	`boolean`	No
`type`	The type of data source. We recommend that you use `CONFLUENCEV2` as your data source type.	`string` The allowed values are `CONFLUENCEV2` and `CONFLUENCE` .	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. **Note** Amazon Q Business crawls identity information from your data source to ensure responses are generated only from documents end users have access to by default. For more information, see Identity crawler.	`boolean`	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string Valid values are FORCED_FULL_CRAWL and FULL_CRAWL. You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index	Yes

Configuration	Description	Type	Required
secretARN	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains the key-value pairs required to connect to your Confluence instance.	string If you use OAuth 2.0 authentication, the secret must contain a JSON structure with the following keys: { "confluenceAppKey": "*client ID for your Confluence account*", "confluenceAppSecret": "*client secret from your Confluence token*", "confluenceAccessToken": "*access token created in Confluence* ", "confluenceRefreshToken": " *refresh token created in Confluence* " } (For Confluence Server/Data Center only) If you use basic authentication, the secret is stored in a JSON structure with the following keys:	Yes

Configuration	Description	Type	Required

		<pre>{
		"username": " *Confluence Server/Data Center username*",
		"password": " *Confluence Server/Data Center password*"
		}</pre>
		(For Confluence Server/Data Center only) If you use Personal Access Token authentication, the secret is stored in a JSON structure with the following keys:
		<pre>{
		"hostUrl": " *Confluence Server/Data Center host URL*",
		"patToken": " *Confluence token*"
		}</pre>	

`version`	The version of this template that's currently supported.	`string`	No

Confluence (Server/Data Center) JSON schema

The following is the Confluence (Server/Data Center) JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["CONFLUENCEV2", "CONFLUENCE"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "sslCertificatePath": {
      "type": "object",
      "properties": {
        "bucket": {
          "type": "string",
          "pattern": "^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$",
          "minLength": 3,
          "maxLength": 63
        },
        "key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 10240
```

```
        }
      },
      "required": ["bucket", "key"]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "hostUrl": {
              "type": "string",
              "pattern": "https:.*"
            },
            "type": {
              "type": "string",
              "enum": ["ON_PREM"]
            },
            "authType": {
              "type": "string",
              "enum": ["Basic", "OAuth2", "Personal-token"]
            }
          },
          "required": ["hostUrl", "type", "authType"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "space": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
```

```
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "page": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
```

```
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "blog": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
```

```
            }
          },
          "required": ["fieldMappings"]
        },
        "comment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "attachment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
```

```
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "isCrawlAcl": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
```

```
          ]
        },
        "fieldForUserId": {
          "type": "string"
        },
        "inclusionSpaceKeyFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionSpaceKeyFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "pageTitleRegEX": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "blogTitleRegEX": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "commentTitleRegEX": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "attachmentTitleRegEX": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "isCrawlPersonalSpace": {
          "anyOf": [
            {
```

```
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlArchivedSpace": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlArchivedPage": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlPage": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlBlog": {
        "anyOf": [
          {
```

```
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlPageComment": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlPageAttachment": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlBlogComment": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlBlogAttachment": {
        "anyOf": [
          {
```

```
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "inclusionFileTypePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionFileTypePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionUrlPatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionUrlPatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "enableDeletionProtection": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
```

```
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "type",
    "syncMode",
    "secretArn",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

Confluence (Server/Data Center) JSON schema example

The following is the Confluence (Server/Data Center) JSON schema example:

```
{
  "type": "CONFLUENCEV2",
  "syncMode": "FULL_CRAWL",
  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-confluence-
secret",
  "enableIdentityCrawler": "true",
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "hostUrl": "https://mycompany.atlassian.net",
      "type": "ON_PREM",
      "authType": "OAuth2"
```

```
    }
  },
  "repositoryConfigurations": {
    "space": {
      "fieldMappings": [
        {
          "indexFieldName": "space_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "page": {
      "fieldMappings": [
        {
          "indexFieldName": "page_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "blog": {
      "fieldMappings": [
        {
          "indexFieldName": "blog_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "comment": {
      "fieldMappings": [
        {
          "indexFieldName": "comment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "attachment": {
```

```
      "fieldMappings": [
        {
          "indexFieldName": "attachment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    }
  },
  "additionalProperties": {
    "isCrawlAcl": "true",
    "fieldForUserId": "user_id",
    "inclusionSpaceKeyFilter": ["SPACE1", "SPACE2"],
    "exclusionSpaceKeyFilter": ["SPACE3"],
    "pageTitleRegEX": ["^.*$"],
    "blogTitleRegEX": ["^.*$"],
    "commentTitleRegEX": ["^.*$"],
    "attachmentTitleRegEX": ["^.*$"],
    "isCrawlPersonalSpace": "false",
    "isCrawlArchivedSpace": "false",
    "isCrawlArchivedPage": "true",
    "isCrawlPage": "true",
    "isCrawlBlog": "true",
    "isCrawlPageComment": "false",
    "isCrawlPageAttachment": "false",
    "isCrawlBlogComment": "true",
    "isCrawlBlogAttachment": "true",
    "maxFileSizeInMegaBytes": "50",
    "inclusionFileTypePatterns": ["*.pdf", "*.docx"],
    "exclusionFileTypePatterns": ["*.tmp"],
    "inclusionUrlPatterns": ["*"],
    "exclusionUrlPatterns": ["*.tmp"],
    "enableDeletionProtection": "false",
    "deletionProtectionThreshold": "15"
  }
}
```

Connecting Amazon Q Business to Confluence (Server/Data Center) using AWS CloudFormation

You use the AWS::QBusiness::DataSource resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- Confluence (Server/Data Center) configuration properties
- Confluence (Server/Data Center) JSON schema for using the configuration property with AWS CloudFormation
- Confluence (Server/Data Center) YAML schema for using the configuration property with AWS CloudFormation

Confluence (Server/Data Center) configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has the following sub-property: `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-properties: `hostUrl`, `type`, and `authType`.	Yes
`hostUrl`	The URL for your Confluence instance. For	`string`	Yes

Configuration	Description	Type	Required
	example, *https://example.confluence.com* . **Important** If you change or update your Confluence (Server/Data Center) data source URL, you also need to update your Secrets Manager secret to ensure a secure connection.	Specify the URL in the pattern `https://*`	
`type`	The hosting method for your Confluence instance.	`string` The allowed values are SAAS or `ON_PREM`.	Yes
`authType`	The authentication method for your Confluence instance.	`string` The allowed values are `Basic`, `OAuth2`, or `Personal-token` .	Yes

Configuration	Description	Type	Required
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties: `space`, `page`, `blog`, `comment`, and `attachment` .	Yes
• `space` • `page` • `blog` • `comment` • `attachment`	A list of objects that map the attributes or field names of your Confluence spaces, pages, blogs, comments, and attachments to Amazon Q index field names.	`object` These properties have the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName` • `dateFieldFormat`	No
`indexFieldName`	The field name of your Confluence spaces, pages, blogs, comments, or attachments.	`string`	Yes
`indexFieldType`	The field type of your Confluence spaces, pages, blogs, comments, or attachments.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes

Configuration	Description	Type	Required
`dataSourceFieldName`	The data source field name of your Confluence spaces, pages, blogs, comments, or attachments.	`string`	Yes
`dateFieldFormat`	The date format of your Confluence spaces, pages, blogs, comments, or attachments.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties. • isCrawlAcl • isRotateSecret • isCrawlPersonalSpace • isCrawlArchivedSpace • isCrawlArchivedPage • isCrawlPage • isCrawlBlog • isCrawlPageComment • isCrawlPageAttachment • isCrawlBlogComment • isCrawlBlogAttachment • fieldForUserId • maxFileSizeInMegaBytes	Yes

Configuration	Description	Type	Required
		• inclusionSpaceKeyFilter • exclusionSpaceKeyFilter • pageTitleRegEX • blogTitleRegEX • commentTitleRegEX • attachmentTitleRegEX • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionUrlPatterns • exclusionUrlPatterns • proxyHost • proxyPort	

Configuration	Description	Type	Required
`isCrawlAcl`	Specify `true` to crawl access control information from documents. **Note** Amazon Q Business crawls ACL information to ensure responses are generated only from documents your end users have access to by default. See Authorization for more details.	`boolean`	No
`isRotateSecret`	Specify `true` if you want to automatically rotate the secret.	`boolean`	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No

Configuration	Description	Type	Required
`proxyHost`	The host where the web proxy is required. The host name should be without protocol (http:// or https://).	`string`	No
`proxyPort`	Port used by the host URL transport protocol. The port number should be a numeric value between 0 and 65535.	`string`	No
`maxFileSizeInMegaBytes`	Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string`	No

Configuration	Description	Type	Required
• inclusionSpaceKeyFilter • exclusionSpaceKeyFilter • pageTitleRegEX • blogTitleRegEX • commentTitleRegEX • attachmentTitleRegEX • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionUrlPatterns • exclusionUrlPatterns	A list of regular expression patterns to include and/or exclude certain files in your Confluence data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.	array (string)	No

Configuration	Description	Type	Required
• `isCrawlPersonalSpace` • `isCrawlArchivedSpace` • `isCrawlArchivedPage` • `isCrawlPage` • `isCrawlBlog` • `isCrawlPageComment` • `isCrawlPageAttachment` • `isCrawlBlogComment` • `isCrawlBlogAttachment`	`true` to index files in your Confluence personal spaces, pages, blogs, page comments, page attachments, blog comments, and blog attachments.	`boolean`	No
`type`	The type of data source. We recommend that you use `CONFLUENCEV2` as your data source type.	`string` The allowed values are `CONFLUENCEV2` and `CONFLUENCE` .	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. **Note** Amazon Q Business crawls identity information from your data source to ensure responses are generated only from documents end users have access to by default. For more information, see Identity crawler.	`boolean`	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string Valid values are FORCED_FULL_CRAWL and FULL_CRAWL. You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index	Yes

Configuration	Description	Type	Required
secretARN	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains the key-value pairs required to connect to your Confluence instance.	string If you use OAuth 2.0 authentication, the secret must contain a JSON structure with the following keys: { "confluenceAppKey": "*client ID for your Confluence account*", "confluenceAppSecret": "*client secret from your Confluence token*", "confluenceAccessToken": "*access token created in Confluence* ", "confluenceRefreshToken": " *refresh token created in Confluence* " } (For Confluence Server/Data Center only) If you use basic authentication, the secret is stored in a JSON structure with the following keys:	Yes

Configuration	Description	Type	Required

		<pre>{
		"username": " *Confluence Server/Data Center username*",
		"password": " *Confluence Server/Data Center password*"
		}</pre>
		(For Confluence Server/Data Center only) If you use Personal Access Token authentication, the secret is stored in a JSON structure with the following keys:
		<pre>{
		"hostUrl": " *Confluence Server/Data Center host URL*",
		"patToken": " *Confluence token*"
		}</pre>	

`version`	The version of this template that's currently supported.	`string`	No

Confluence (Server/Data Center) JSON schema for using the configuration property with AWS CloudFormation

The following is the Confluence (Server/Data Center) JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- Confluence (Server/Data Center) JSON schema for using the configuration property with AWS CloudFormation
- Confluence (Server/Data Center) JSON schema example for using the configuration property with AWS CloudFormation

Confluence (Server/Data Center) JSON schema for using the configuration property with AWS CloudFormation

The following is the Confluence (Server/Data Center) JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["CONFLUENCEV2", "CONFLUENCE"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
```

```
          "enum": ["true", "false"]
        }
      ]
    },
    "sslCertificatePath": {
      "type": "object",
      "properties": {
        "bucket": {
          "type": "string",
          "pattern": "^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$",
          "minLength": 3,
          "maxLength": 63
        },
        "key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 10240
        }
      },
      "required": ["bucket", "key"]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "hostUrl": {
              "type": "string",
              "pattern": "https:.*"
            },
            "type": {
              "type": "string",
              "enum": ["ON_PREM"]
            },
            "authType": {
              "type": "string",
              "enum": ["Basic", "OAuth2", "Personal-token"]
            }
          },
          "required": ["hostUrl", "type", "authType"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
```

```
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "space": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "page": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
```

```
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "blog": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
```

```
                    "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "comment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
```

```
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "attachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
```

```
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "isCrawlAcl": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "fieldForUserId": {
        "type": "string"
      },
      "inclusionSpaceKeyFilter": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionSpaceKeyFilter": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "pageTitleRegEX": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "blogTitleRegEX": {
        "type": "array",
        "items": {
          "type": "string"
```

```
        }
      },
      "commentTitleRegEX": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "attachmentTitleRegEX": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "isCrawlPersonalSpace": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlArchivedSpace": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlArchivedPage": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
```

```
            }
          ]
        },
        "isCrawlPage": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlBlog": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlPageComment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlPageAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
```

```
            }
          ]
        },
        "isCrawlBlogComment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlBlogAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionUrlPatterns": {
          "type": "array",
          "items": {
            "type": "string"
```

```
          }
        },
        "exclusionUrlPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "type",
    "syncMode",
    "secretArn",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
```

```
}
```

Confluence (Server/Data Center) JSON schema example for using the configuration property with AWS CloudFormation

The following is the Confluence (Server/Data Center) JSON schema example for the configuration property for CloudFormation

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation CONFLUENCE Data Source Template",
  "Resources": {
    "DataSourceConfluence": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MyConfluenceDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "CONFLUENCEV2",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-
confluence-secret",
          "enableIdentityCrawler": "true",
          "sslCertificatePath": {
            "bucket": "my-confluence-bucket",
            "key": "path/to/certificate.pem"
          },
          "connectionConfiguration": {
            "repositoryEndpointMetadata": {
              "hostUrl": "https://mycompany.atlassian.net",
              "type": "ON_PREM",
              "authType": "Personal-token"
            }
          },
          "repositoryConfigurations": {
            "space": {
              "fieldMappings": [
                {
                  "indexFieldName": "space_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
```

```
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "page": {
        "fieldMappings": [
          {
            "indexFieldName": "page_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "blog": {
        "fieldMappings": [
          {
            "indexFieldName": "blog_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "comment": {
        "fieldMappings": [
          {
            "indexFieldName": "comment_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "attachment": {
        "fieldMappings": [
          {
            "indexFieldName": "attachment_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      }
```

```
          },
          "additionalProperties": {
            "isCrawlAcl": "true",
            "fieldForUserId": "user_id",
            "inclusionSpaceKeyFilter": ["SPACE1", "SPACE2"],
            "exclusionSpaceKeyFilter": ["SPACE3"],
            "pageTitleRegEX": ["^.*$"],
            "blogTitleRegEX": ["^.*$"],
            "commentTitleRegEX": ["^.*$"],
            "attachmentTitleRegEX": ["^.*$"],
            "isCrawlPersonalSpace": "false",
            "isCrawlArchivedSpace": "false",
            "isCrawlArchivedPage": "true",
            "isCrawlPage": "true",
            "isCrawlBlog": "true",
            "isCrawlPageComment": "false",
            "isCrawlPageAttachment": "false",
            "isCrawlBlogComment": "true",
            "isCrawlBlogAttachment": "true",
            "maxFileSizeInMegaBytes": "50",
            "inclusionFileTypePatterns": ["*.pdf", "*.docx"],
            "exclusionFileTypePatterns": ["*.tmp"],
            "inclusionUrlPatterns": ["*"],
            "exclusionUrlPatterns": ["*.tmp"],
            "enableDeletionProtection": "false",
            "deletionProtectionThreshold": "15"
          }
        }
      }
    }
  }
}
```

Confluence (Server/Data Center) YAML schema for using the configuration property with AWS CloudFormation

The following is the Confluence (Server/Data Center) YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- Confluence (Server/Data Center) YAML schema for using the configuration property with AWS CloudFormation

- Confluence (Server/Data Center) YAML schema example for using the configuration property with AWS CloudFormation

Confluence (Server/Data Center) YAML schema for using the configuration property with AWS CloudFormation

The following is the Confluence (Server/Data Center) YAML schema for the configuration property for CloudFormation.

```
AWSTemplateFormatVersion: "2010-09-09"
Description: CloudFormation CONFLUENCE Data Source Template
Resources:
  DataSourceConfluence:
    Type: AWS::QBusiness::DataSource
    Properties:
      ApplicationId: app12345-1234-1234-1234-123456789012
      IndexId: indx1234-1234-1234-1234-123456789012
      DisplayName: MyConfluenceDataSource
      RoleArn: arn:aws:iam::123456789012:role/qbusiness-data-source-role
      Configuration:
        type: CONFLUENCEV2
        syncMode: FULL_CRAWL
        secretArn: arn:aws:secretsmanager:us-west-2:123456789012:secret:my-confluence-
secret
        enableIdentityCrawler: "true"
        sslCertificatePath:
          bucket: my-confluence-bucket
          key: path/to/certificate.pem
        connectionConfiguration:
          repositoryEndpointMetadata:
            hostUrl: https://mycompany.atlassian.net
            type: ON_PREM
            authType: Personal-token
        repositoryConfigurations:
          space:
            fieldMappings:
              - indexFieldName: space_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
          page:
            fieldMappings:
```

```
            - indexFieldName: page_id
              indexFieldType: STRING
              dataSourceFieldName: id
              dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
        blog:
          fieldMappings:
            - indexFieldName: blog_id
              indexFieldType: STRING
              dataSourceFieldName: id
              dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
        comment:
          fieldMappings:
            - indexFieldName: comment_id
              indexFieldType: STRING
              dataSourceFieldName: id
              dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
        attachment:
          fieldMappings:
            - indexFieldName: attachment_id
              indexFieldType: STRING
              dataSourceFieldName: id
              dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
      additionalProperties:
        isCrawlAcl: "true"
        fieldForUserId: user_id
        inclusionSpaceKeyFilter:
          - SPACE1
          - SPACE2
        exclusionSpaceKeyFilter:
          - SPACE3
        pageTitleRegEX:
          - "^.*$"
        blogTitleRegEX:
          - "^.*$"
        commentTitleRegEX:
          - "^.*$"
        attachmentTitleRegEX:
          - "^.*$"
        isCrawlPersonalSpace: "false"
        isCrawlArchivedSpace: "false"
        isCrawlArchivedPage: "true"
        isCrawlPage: "true"
        isCrawlBlog: "true"
        isCrawlPageComment: "false"
```

```
          isCrawlPageAttachment: "false"
          isCrawlBlogComment: "true"
          isCrawlBlogAttachment: "true"
          maxFileSizeInMegaBytes: "50"
          inclusionFileTypePatterns:
            - "*.pdf"
            - "*.docx"
          exclusionFileTypePatterns:
            - "*.tmp"
          inclusionUrlPatterns:
            - "*"
          exclusionUrlPatterns:
            - "*.tmp"
          enableDeletionProtection: "false"
          deletionProtectionThreshold: "15"
```

Confluence (Server/Data Center) YAML schema example for using the configuration property with AWS CloudFormation

The following is the Confluence (Server/Data Center) YAML example for the Configuration property for CloudFormation:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: CloudFormation CONFLUENCE Data Source Template
Resources:
  DataSourceConfluence:
    Type: AWS::QBusiness::DataSource
    Properties:
      ApplicationId: app12345-1234-1234-1234-123456789012
      IndexId: indx1234-1234-1234-1234-123456789012
      DisplayName: MyConfluenceDataSource
      RoleArn: arn:aws:iam::123456789012:role/qbusiness-data-source-role
      Configuration:
        type: CONFLUENCEV2
        syncMode: FULL_CRAWL
        secretArn: arn:aws:secretsmanager:us-west-2:123456789012:secret:my-confluence-
secret
        enableIdentityCrawler: "true"
        sslCertificatePath:
          bucket: my-confluence-bucket
          key: path/to/certificate.pem
        connectionConfiguration:
          repositoryEndpointMetadata:
```

```
    hostUrl: https://mycompany.atlassian.net
    type: ON_PREM
    authType: Personal-token
repositoryConfigurations:
  space:
    fieldMappings:
      - indexFieldName: space_id
        indexFieldType: STRING
        dataSourceFieldName: id
        dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
  page:
    fieldMappings:
      - indexFieldName: page_id
        indexFieldType: STRING
        dataSourceFieldName: id
        dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
  blog:
    fieldMappings:
      - indexFieldName: blog_id
        indexFieldType: STRING
        dataSourceFieldName: id
        dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
  comment:
    fieldMappings:
      - indexFieldName: comment_id
        indexFieldType: STRING
        dataSourceFieldName: id
        dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
  attachment:
    fieldMappings:
      - indexFieldName: attachment_id
        indexFieldType: STRING
        dataSourceFieldName: id
        dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
additionalProperties:
  isCrawlAcl: "true"
  fieldForUserId: user_id
  inclusionSpaceKeyFilter:
    - SPACE1
    - SPACE2
  exclusionSpaceKeyFilter:
    - SPACE3
  pageTitleRegEX:
    - "^.*$"
```

```
          blogTitleRegEX:
            - "^.*$"
          commentTitleRegEX:
            - "^.*$"
          attachmentTitleRegEX:
            - "^.*$"
          isCrawlPersonalSpace: "false"
          isCrawlArchivedSpace: "false"
          isCrawlArchivedPage: "true"
          isCrawlPage: "true"
          isCrawlBlog: "true"
          isCrawlPageComment: "false"
          isCrawlPageAttachment: "false"
          isCrawlBlogComment: "true"
          isCrawlBlogAttachment: "true"
          maxFileSizeInMegaBytes: "50"
          inclusionFileTypePatterns:
            - "*.pdf"
            - "*.docx"
          exclusionFileTypePatterns:
            - "*.tmp"
          inclusionUrlPatterns:
            - "*"
          exclusionUrlPatterns:
            - "*.tmp"
          enableDeletionProtection: "false"
          deletionProtectionThreshold: "15"
```

How Amazon Q Business connector crawls Confluence (Server/Data Center) ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect a Confluence (Server/Data Center) data source to Amazon Q Business, Amazon Q crawls ACL information attached to a document (user and group information) from your Confluence (Server/Data Center) instance. If you choose to activate ACL crawling, the information can be used to filter chat responses based on your end users' document access level.

The connector crawls the following Confluence resources:

- **Spaces** – A collection of related pages, blogs, and attachments. Space permissions apply to all documents in the space by default.
- **Pages** – Documents in a space where users create and manage content. Pages can contain text, images, tables, and multimedia elements, and can have nested pages. Each page is considered a single document. Pages can be restricted to specific users and groups in the space. A nested page inherits restrictions from the parent page, and can have its own restrictions.
- **Blogs** – Content similar to pages, typically used for updates or announcements. Each blog post is considered as a single document. Blogs can be restricted to specific users and groups in the space.
- **Comments** – Feedback and discussions on pages or blog post content. Comments are visible to viewers of the page or post.
- **Attachments** – Files uploaded to pages or blog posts, such as images and documents.

The connector also crawls user principal information (local user alias, local group and federated group identity configurations) and its permissions for each configured space. The Confluence (Server/Data Center) connector does not support crawling macros, whiteboards, or databases.

The connector updates ACL changes each time it crawls your data source content. To ensure that the correct users have access to the correct content, regularly re-sync your data source to capture any ACL updates.

You configure user and group access to spaces using the space permissions page. For pages and blogs, you use the restrictions page. For more information about space permissions, see Space Permissions Overview on the Confluence Support website. For more information about page and blog restrictions, see Page Restrictions on the Confluence Support website.

> **Important**
>
> For user context filtering to work correctly, users' visibility must be set to **Anyone**. For more information, see Set your email visibility in Atlassian Developer Documentation.

The group and user IDs are mapped as follows:

- `_group_ids` – Group names are present on spaces, pages, and blogs where there are restrictions. They're mapped from the name of the group in Confluence . Group names are always lower case.

- `_user_id` – User names are present on the space, page, or blog where there are restrictions. They're mapped depending on the type of Confluence instance that you are using.
- For Confluence (Server/Data Center) – The `_user_id` is the user key of the user.

> **Important**
>
> To maintain secure access control for Amazon Q Business, each user must have a unique email address across all connected data sources.
> In Confluence Data Center users can share an email address while having a different application-specific unique identifier. However, in Amazon Q Business email addresses act as unique identifiers.
> This means that if a document is shared with a particular user (for example, arnav_desai@example.com who is part of pentesters@example.com) on the basis of an application-specific unique ID, every other user who shares pentesters@example.com (for example, xiulan_wang@example.com and efua_owusu@example.com, both of whom are part of pentesters@example.com) can receive Amazon Q Business responses with content from a document that was shared only with Arnav. Similarly, content created by Arnav that only he should be able to access via Amazon Q Business chat responses, could also be part of Amazon Q Business chat responses for Xiulan and Efua, because they share the same email address.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Amazon Q Business Confluence (Server/Data Center) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application environment and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Confluence connector supports the following entities and the associated reserved and custom attributes.

> **Important**
>
> If you map any Confluence (Server/Data Center) field to Amazon Q document title and document body fields, Amazon Q will generate responses from data in the document title and body.

Supported entities and field mappings

- Space
- Page
- Blog
- Comment
- Attachment

Space

Confluence field name	Index field name	Description	Data type
spaceName	cf_sp_document_title	Custom	String
itemType	_category	Default	String
url	_source_uri	Default	String
spaceKey	cf_space_key	Custom	String
description	cf_description	Custom	String
spaceType	cf_type	Custom	String

Page

Confluence field name	Index field name	Description	Data type
title	_cf_page_document_title	Custom	String
authors	_authors	Default	String list
createdDate	_created_at	Default	Date
modifiedDate	_last_updated_at	Default	Date
labels	cf_labels	Custom	String list
version	cf_version	Custom	Long (numeric)
itemType	_category	Default	String
spaceKey	cf_space_key	Custom	String
spaceName	cf_space_name	Custom	String

Confluence field name	Index field name	Description	Data type
url	_source_uri	Default	String
status	cf_status	Custom	String
parentId	cf_parent_id	Custom	String

Blog

Confluence field name	Index field name	Description	Data type
title	cf_bg_document_title	Custom	String
author	_authors	Default	String list
publishedDate	_created_at	Default	Date
labels	_source_uri	Default	String
version	cf_version	Custom	Long (numeric)
itemType	_category	Custom	String
spaceKey	cf_space_key	Custom	String
modifiedDate	_last_updated_at	Default	Date
spaceName	cf_space_name	Custom	String
status	cf_status	Custom	String
url	_source_uri	Default	String
parentId	cf_parent_id	Custom	String

Comment

Confluence field name	Index field name	Description	Data type
title	cf_cmt_document_title	Custom	String
author	_authors	Default	String list
createdDate	_created_at	Default	Date
version	cf_version	Custom	Long (numeric)
itemType	_category	Default	String
spaceKey	cf_space_key	Custom	String
spaceName	cf_space_name	Custom	String
contentType	cf_content_type	Custom	String
url	_source_uri	Default	String
parentId	cf_parent_id	Custom	String
status	cf_status	Custom	String

Attachment

Confluence field name	Index field name	Description	Data type
fileName	cf_attachment_document_title	Custom	String
author	_authors	Default	String list
createdDate	_created_at	Default	Date

Confluence field name	Index field name	Description	Data type
labels	cf_labels	Custom	String list
version	cf_version	Custom	Long (numeric)
itemType	_category	Default	String
spaceKey	cf_space_key	Custom	String
contentType	cf_content_type	Custom	String
modifiedDate	_last_updated_at	Default	Date
fileSize	cf_file_size	Custom	Long (numeric)
fileType	cf_attachment_file_type	Custom	String
spaceName	cf_space_name	Custom	String
documentId	_document_id	Default	String list
url	_source_uri	Default	String
parentId	cf_parent_id	Custom	String
attachmentComment	cf_attachment_comment	Custom	String
status	cf_status	Custom	String

IAM role for Amazon Q Confluence (Server/Data Center) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
```

```
            ]
        },
        {
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the Amazon Q Business Confluence (Server/Data Center) connector

The following table provides information about error codes you may see for the Confluence (Server/Data Center) connector and suggested resolutions.

Error code	Error message	Suggested resolution
CNF-5500	Null/empty username.	Provide username.
CNF-5501	Error validating credentials due to Invalid username or password.	Provide valid username/password
CNF-5502	Null/empty confluence AppKey.	Provide confluence AppKey.

Error code	Error message	Suggested resolution
CNF-5503	Null/empty confluence Secret.	Provide confluence Secret.
CNF-5504	Null/empty Client Access Token.	Provide Client Access Token.
CNF-5505	Null/empty Client Refresh Token	Provide Client Refresh Token
CNF-5506	Incorrect auth type.	Auth type should be Basic or OAuth2 or Personal-token.
CNF-5507	Null/empty auth type.	Auth Type should not be null or empty value.
CNF-5508	Empty/null host URL.	Host Url should not be null or empty value.
CNF-5509	Null/empty crawl type.	Crawl Type should not be null or empty value.
CNF-5510	Null/empty Repository Configurations.	Repository Configurations should not be null or empty value.
CNF-5511	Incorrect type.	type should be SAAS or ON_PREM.
CNF-5512	Invalid inclusion file type patterns.	Provide the correct inclusion patterns.
CNF-5513	Invalid exclusion file type patterns.	Provide the correct exclusion patterns.
CNF-5514	Invalid regex patterns.	Provide the correct regex patterns.
CNF-5515	Error validating credentia ls due to invalid username or password.	Provide valid username and password.

Error code	Error message	Suggested resolution
CNF-5516	Error validating credentials due to invalid client id or client secret.	Provide valid client id and client secret.
CNF-5517	Error validating crawl type.	Provide valid crawl type.
CNF-5518	Invalid URI.	Provide valid URI.
CNF-5519	Null/empty DataSourceFieldName in Space Entity.	Provide value for DataSourceFieldName in Space Entity.
CNF-5520	Null/empty IndexFieldName in Blog Entity.	Provide value for IndexFieldName in Blog Entity.
CNF-5521	Null/empty IndexFieldType in Space Entity.	Provide value for IndexFieldType in Space Entity.
CNF-5522	Null/empty password.	Provide password.
CNF-5523	Incorrect auth type.	Auth type should be Basic or OAuth2.
CNF-5524	Null/empty DataSourceFieldName in Page Entity.	Provide value for DataSourceFieldName in Page Entity.
CNF-5525	Null/empty DataSourceFieldName in Blog Entity	Please provide value for DataSourceFieldName in Blog Entity
CNF-5526	Null/empty DataSourceFieldName in Comment Entity.	Provide value for DataSourceFieldName in Comment Entity.

Error code	Error message	Suggested resolution
CNF-5527	Null/empty DataSourceFieldName in Attachment Entity.	Provide value for DataSourceFieldName in Attachment Entity.
CNF-5528	Null/empty IndexFieldName.	IndexFieldName field can't be null or empty value.
CNF-5529	Null/empty IndexFieldName in Space Entity.	Provide value for IndexFieldName in Space Entity.
CNF-5530	Null/empty IndexFieldName in Page Entity	Please provide value for IndexFieldName in Page Entity
CNF-5531	Invalid isCrawlPersonalSpace value.	isCrawlPersonalSpace should be a boolean value true or false.
CNF-5532	Invalid isCrawlArchivedSpace value.	isCrawlArchivedSpace should be a boolean value true or false.
CNF-5533	Invalid isCrawlArchivedPage value.	isCrawlArchivedPage should be a boolean value true or false.
CNF-5534	Invalid isCrawlPage value.	isCrawlPage should be a boolean value true or false.
CNF-5535	Invalid isCrawlBlogComment value.	isCrawlBlogComment should be a boolean value true or false.
CNF-5536	Invalid isCrawlBlogComment value.	isCrawlBlogComment should be a boolean value true or false.
CNF-5537	Invalid isCrawlBlogAttachment value.	isCrawlBlogAttachment should be a boolean value true or false.
CNF-5538	Error validating on protocol.	Provide valid protocol.

Error code	Error message	Suggested resolution
CNF-5539	Null/empty IndexFiel dName in Comment Entity.	Provide value for IndexFieldName in Comment Entity.
CNF-5540	Null/empty Personal Access Token.	Provide Personal Access Token.
CNF-5541	Invalid OAuth value.	Give a valid OAuth URL.
CNF-5542	Invalid Space value.	Give a valid Space URL.
CNF-5543	Archived Space Exception .	Check Archived Space.
CNF-5544	JSON Exception for Space.	Check Space.
CNF-5545	JSON Exception for Comment.	Check Comment.
CNF-5546	JSON Exception for Comment.	Check Comment.
CNF-5547	JSON Exception for Comment.	Check Comment.
CNF-5548	JSON Exception for Attachment.	Check Attachment.
CNF-5549	JSON Exception for Blog.	Check Blog.
CNF-5550	JSON Exception for Page.	Check Page.
CNF-5551	JSON Exception for Label.	Check Label.
CNF-5552	JSON Exception for ACL.	Check ACL.

Error code	Error message	Suggested resolution
CNF-5553	JSON Exception for Groups.	Check Groups.
CNF-5554	JSON Exception for Group Members.	Check Group Members.
CNF-5555	JSON Exception for Space Group.	Check Space Group.
CNF-5556	Exception in CommentItem.	Check the CommentItem class.
CNF-5557	Invalid isCrawlPageComment value.	isCrawlPageComment should be a boolean value true or false.
CNF-5558	Invalid isCrawlPageAttachment value.	isCrawlPageAttachment should be a boolean value true or false.
CNF-5559	Null/empty Repository Configurations.	Repository Configurations should not be null or empty value.
CNF-5560	Null/empty IndexFieldName in Attachment.	Please provide value for IndexFieldName in Attachment Entity.
CNF-5561	Invalid proxy url.	Proxy url should not contain http: or https.
CNF-5562	Null/Empty proxy port.	Provide a valid proxy port.
CNF-5563	Invalid Host URL.	Provide valid Host URL.
CNF-5564	Invalid proxy port value.	Provide a valid proxy port.
CNF-5565	Confluence server not reachable.	Provide a valid proxy and server details.
CNF-5566	Null/empty IndexFieldType in Page Entity.	Provide value for IndexFieldType in Page Entity.

Error code	Error message	Suggested resolution
CNF-5567	Null/empty IndexFiel dType in Blog Entity.	Provide value for IndexFieldType in Blog Entity.
CNF-5568	Null/empty IndexFiel dType in Comment Entity.	Provide value for IndexFieldType in Comment Entity.
CNF-5569	Null/empty IndexFiel dType in Attachment.	Provide value for IndexFieldType in Attachment. Entity
CNF-5570	JSON Exception for Content Ancestors.	Check your Ancestors.
CNF-5571	Invalid Host URL Pattern.	Provide valid Host URL Pattern.
CNF-5572	Error validating credentia ls due to Invalid access or refresh token.	Invalid AccessToken/RefreshToken.

Connecting Dropbox to Amazon Q Business

Dropbox is a file hosting service that offers cloud storage, document organization, and document templating services. You can connect Dropbox instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the Dropbox connector
- Dropbox connector overview
- Prerequisites for connecting Amazon Q Business to Dropbox
- Connecting Amazon Q Business to Dropbox using the console
- Connecting Amazon Q Business to Dropbox using APIs
- How Amazon Q Business connector crawls Dropbox ACLs
- Dropbox data source connector field mappings
- IAM role for Dropbox connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Dropbox connector

The Dropbox connector has the following known limitations:

- When Access Control Lists (ACLs) are enabled, the "Sync only new or modified content" option is not available due to Dropbox API limitations. We recommend using "Full sync" or "New, modified, or deleted content sync" modes instead, or disable ACLs if you need to use this sync mode.

Dropbox connector overview

The following table gives an overview of the Amazon Q Business Dropbox connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	OAuth 2.0 short-lived access token and refresh token (offline access)
	Authentication credentials	OAuth 2.0 short-lived access token and refresh token (offline access) • App key • App secret • Access token • Refresh token (recommended)

Category	Feature	Support
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Files • Dropbox Paper • Dropbox Paper Templates • Shortcuts See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include/ exclude **Files Dropbox Paper**, **Dropbox Paper templates**, and **Shortcuts**. • Include/exclude content by file name, file type, and file path.
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Dropbox

Before you begin, make sure that you have completed the following prerequisites.

In Dropbox, make sure you have:

- Created a Dropbox Advanced account and set up an admin user.
- Created a Dropbox app with a unique **App name**, activated **Scoped Access**. For more information, see Dropbox documentation on creating an app on the Dropbox website.
- Activated **Full Dropbox** permissions on the Dropbox console and added the following permissions:
  - `files.content.read`
  - `files.metadata.read`
  - `sharing.read`
  - `file_requests.read`
  - `groups.read`
  - `team_info.read`
  - `team_data.content.read`
  - `account_info.read`
  - `members.read`
  - `team_data.member`
- Create an authorization URL containing client ID (app-key), redirect_uri, response type, access type and scopes. Obtain User Authorization by signing in to Dropbox and grant your application the requested permissions.

  ```
  Sample Authorization URL:

  https://www.dropbox.com/oauth2/authorize

  ?client_id=abcd1234example

  &redirect_uri=https%3A%2F%2Fyourapp.com%2Fcallback

  &response_type=code

  &token_access_type=offline
  ```

```
&scope=files.metadata.read%20files.content.read
```

- Exchange authorization code for tokens by requesting tokens from the Dropbox token endpoint.
  - curl https://api.dropboxapi.com/oauth2/token -d code=AUTH_CODE -d grant_type=authorization_code -d client_id=APP_KEY -d client_secret=APP_SECRET
  - Replace AUTH_CODE with the obtained authorization code, APP_KEY and APP_SECRET with your application client ID (App key) and secret key.
- Noted your Dropbox app key, Dropbox app secret, and Dropbox access token and refresh token for OAuth 2.0 authentication credentials.
- Generate an OAuth 2.0 access token with token_access_type=offline to obtain a short-lived access token and a long-lived refresh token. For more information, see Dropbox documentation on OAuth authentication on the Dropbox website.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Dropbox authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Dropbox using the console

The following procedure outlines how to connect Amazon Q Business to Dropbox using the AWS Management Console.

Connecting Amazon Q to Dropbox

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Dropbox** data source to your Amazon Q application.
5. Then, on the **Dropbox** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
8. In **Authentication** – OAuth 2.0 (offline access) is supported. You must provide App key, App secret, access token, and refresh token.
9. In **Authentication credentials**, for **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your Dropbox authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens.

   - Enter following information in the **Create an AWS Secrets Manager secret window**:

     i. **Secret name** – A name for your secret.

     ii. For **App key**, **App secret**, **access token** and **refresh token** – Enter the authentication credential values that you generated from your Dropbox account.

     iii. Choose **Save**.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **Identity crawler** – Amazon Q crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.

12. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.

13. In **Sync scope**, enter the following information.

    a. For **Select entities or content types** – Choose entities or content types you want to crawl.

    b. **Change log mode** – Choose to update your index instead of syncing all files.

    c. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

    d. In **Additional configuration – *optional***, for **Regex patterns** – Add regular expression patterns to include or exclude certain files.

    e. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete

phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
15. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
16. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

17. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.

You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Dropbox using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Dropbox JSON schema

The following is the Dropbox JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
          }
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
```

```
        "file": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": {
                "anyOf": [
                  {
                    "type": "object",
                    "properties": {
                      "indexFieldName": {
                        "type": "string"
                      },
                      "indexFieldType": {
                        "type": "string",
                        "enum": [
                          "STRING",
                          "STRING_LIST",
                          "LONG",
                          "DATE"
                        ]
                      },
                      "dataSourceFieldName": {
                        "type": "string"
                      },
                      "dateFieldFormat": {
                        "type": "string",
                        "pattern": "dd-MM-yyyy HH:mm:ss"
                      }
                    },
                    "required": [
                      "indexFieldName",
                      "indexFieldType",
                      "dataSourceFieldName"
                    ]
                  }
                ]
              }
            }
          },
          "required": [
            "fieldMappings"
          ]
        },
```

```
        "paper": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": {
                "anyOf": [
                  {
                    "type": "object",
                    "properties": {
                      "indexFieldName": {
                        "type": "string"
                      },
                      "indexFieldType": {
                        "type": "string",
                        "enum": [
                          "STRING",
                          "STRING_LIST",
                          "LONG",
                          "DATE"
                        ]
                      },
                      "dataSourceFieldName": {
                        "type": "string"
                      },
                      "dateFieldFormat": {
                        "type": "string",
                        "pattern": "dd-MM-yyyy HH:mm:ss"
                      }
                    },
                    "required": [
                      "indexFieldName",
                      "indexFieldType",
                      "dataSourceFieldName"
                    ]
                  }
                ]
              }
            }
          },
          "required": [
            "fieldMappings"
          ]
        },
```

```
        "papert": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": {
                "anyOf": [
                  {
                    "type": "object",
                    "properties": {
                      "indexFieldName": {
                        "type": "string"
                      },
                      "indexFieldType": {
                        "type": "string",
                        "enum": [
                          "STRING",
                          "STRING_LIST",
                          "LONG",
                          "DATE"
                        ]
                      },
                      "dataSourceFieldName": {
                        "type": "string"
                      },
                      "dateFieldFormat": {
                        "type": "string",
                        "pattern": "dd-MM-yyyy HH:mm:ss"
                      }
                    },
                    "required": [
                      "indexFieldName",
                      "indexFieldType",
                      "dataSourceFieldName"
                    ]
                  }
                ]
              }
            }
          },
          "required": [
            "fieldMappings"
          ]
        },
```

```
        "shortcut": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": {
                "anyOf": [
                  {
                    "type": "object",
                    "properties": {
                      "indexFieldName": {
                        "type": "string"
                      },
                      "indexFieldType": {
                        "type": "string",
                        "enum": [
                          "STRING",
                          "STRING_LIST",
                          "LONG",
                          "DATE"
                        ]
                      },
                      "dataSourceFieldName": {
                        "type": "string"
                      },
                      "dateFieldFormat": {
                        "type": "string",
                        "pattern": "dd-MM-yyyy HH:mm:ss"
                      }
                    },
                    "required": [
                      "indexFieldName",
                      "indexFieldType",
                      "dataSourceFieldName"
                    ]
                  }
                ]
              }
            }
          },
          "required": [
            "fieldMappings"
          ]
        }
```

```
      }
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "type": "boolean"
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "isCrawlAcl": {
          "type": "boolean"
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        },
        "fieldForUserId": {
          "type": "string"
        },
        "inclusionPatterns": {
          "type": "array"
        },
        "exclusionPatterns": {
          "type": "array"
        },
        "crawlFile": {
          "type": "boolean"
        },
        "crawlPaper": {
          "type": "boolean"
        },
        "crawlPapert": {
          "type": "boolean"
        },
        "crawlShortcut": {
          "type": "boolean"
        }
      }
    },
    "type": {
      "type": "string",
```

```
      "pattern": "DROPBOX"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FULL_CRAWL",
        "FORCED_FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "additionalProperties": false,
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties",
    "syncMode",
    "secretArn",
    "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the endpoint for the data source.
`repositoryEndpointMetadata`	The endpoint information for the data source. This data source doesn't specify an endpoint in `repositoryEndpointMetadata` . Rather, the connection information is included in an

Configuration	Description
	AWS Secrets Manager secret that you provide the `secretArn` .
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.
• `file` • `paper` • `papert` • `shortcut`	A list of objects that map the attributes or field names of your Dropbox files, Dropbox Paper, and shortcuts to Amazon Q index field names.
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/principal informati on on users and groups with access to specific documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.

Configuration	Description
secretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Dropbox. The secret must contain a JSON structure with the following keys: `{ "appKey": "Dropbox app key", "appSecret": "Dropbox app secret", "accesstoken": "access token (short live)", "refreshtoken": "refresh token (offline-access)" }`
additionalProperties	Additional configuration options for your content in your data source.
maxFileSizeInMegaBytes	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
isCrawlAcl	Specify `true` to crawl access control informati on from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.

Configuration	Description
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.
`inclusionFileTypePatterns`	A list of regular expression patterns to *include* specific file types in your Dropbox data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.
`exclusionFileTypePatterns`	A list of regular expression patterns to *exclude* specific file types in your Dropbox data source. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an exclusion and inclusion pattern, the exclusion pattern takes precedenc e and the file isn't included in the index.
`exclusionFileNamePatterns`	A list of regular expression patterns to *exclude* specific file names in your Dropbox data source. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an exclusion and inclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.

Configuration	Description
`exclusionFileNamePatterns`	A list of regular expression patterns to *exclude* specific file names in your Dropbox data source. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an exclusion and inclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.
• `crawlFile` • `crawlPaper` • `crawlPapert` • `crawlShortcut`	`true` to index files in your Dropbox, Dropbox Paper documents, Dropbox Paper templates , and webpage shortcuts stored in your Dropbox.
`type`	The type of data source. Specify `DROPBOX` as your data source type.
`useChangeLog`	`true` to use the Dropbox change log to determine which documents require adding, updating, or deleting in the index. Depending on the change log's size, it may take longer for Amazon Q to use the change log than to scan all of your documents in your Dropbox.
`version`	The version of this template that's currently supported.

How Amazon Q Business connector crawls Dropbox ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an Dropbox data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your Dropbox instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

The group and user IDs are mapped as follows:

- `_group_ids` – Group IDs exist in Dropbox on files where there are set access permissions. They're mapped from the names of the groups in Dropbox.
- `_user_id` – User IDs exist in Dropbox on files where there are set access permissions. They're mapped from the user emails as the IDs in Dropbox.

For more information, see:

- Authorization
- Identity crawler

Dropbox data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Dropbox connector supports the following entities and the associated reserved and custom attributes.

Supported entities and field mappings

- Files
- Dropbox Paper
- Dropbox Paper Templates
- Shortcuts

Files

Dropbox field name	Index field name	Description	Data type
sourceUrl	_source_uri	Default	String
category	_category	Default	String
fileName	dbx_file_name	Custom	String
fileId	dbx_id1	Custom	String
clientModifiedDate	dbx_client_modified	Custom	Date
serverModifiedDate	dbx_server_modified	Custom	Date
fileSize	dbx_file_size	Custom	Long (numeric)
pathDisplay	dbx_path_display	Custom	String
tags	dbx_tags	Custom	String

Dropbox Paper

Dropbox field name	Index field name	Description	Data type
sourceUrl	_source_uri	Default	String
category	_category	Default	String
fileName	dbx_file_name	Custom	String
fileId	dbx_id1	Custom	String
clientModifiedDate	dbx_client_modified	Custom	Date
serverModifiedDate	dbx_server_modified	Custom	Date
fileSize	dbx_file_size	Custom	Long (numeric)
pathDisplay	dbx_path_display	Custom	String
tags	dbx_tags	Custom	String

Dropbox Paper Templates

Dropbox field name	Index field name	Description	Data type
sourceUrl	_source_uri	Default	String
category	_category	Default	String
fileName	dbx_file_name	Custom	String
fileId	dbx_id1	Custom	String
clientModifiedDate	dbx_client_modified	Custom	Date
serverModifiedDate	dbx_server_modified	Custom	Date
fileSize	dbx_file_size	Custom	Long (numeric)

Dropbox field name	Index field name	Description	Data type
pathDisplay	dbx_path_display	Custom	String
tags	dbx_tags	Custom	String

Shortcuts

Dropbox field name	Index field name	Description	Data type
sourceUrl	_source_uri	Default	String
category	_category	Default	String
fileName	dbx_file_name	Custom	String
fileId	dbx_id1	Custom	String
clientModifiedDate	dbx_client_modified	Custom	Date
serverModifiedDate	dbx_server_modified	Custom	Date
fileSize	dbx_file_size	Custom	Long (numeric)
pathDisplay	dbx_path_display	Custom	String
tags	dbx_tags	Custom	String

IAM role for Dropbox connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
```

```
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
```

```
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Amazon FSx (Windows) to Amazon Q Business

Amazon FSx (Windows) is a fully managed, cloud based file server system that offers shared storage capabilities. You can connect your Amazon FSx (Windows) instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

The Amazon Q Amazon FSx (Windows) data source connector supports only Amazon FSx for Windows.

Topics

- Amazon FSx (Windows) connector overview
- Prerequisites for connecting Amazon Q Business to Amazon FSx (Windows)
- Connecting Amazon Q Business to Amazon FSx (Windows) using the console
- Connecting Amazon Q Business to Amazon FSx (Windows) using APIs
- How Amazon Q Business connector crawls Amazon FSx (Windows) ACLs
- Amazon FSx (Windows) data source connector field mappings
- IAM role for Amazon FSx (Windows) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Amazon FSx (Windows) connector overview

The following table gives an overview of the Amazon FSx (Windows) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Ad Server authentication
	Authentication credentials	• Amazon FSx (Windows) username • Amazon FSx (Windows) password
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	No
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include/exclude by file name • Include/exclude by file type • Include/exclude by file path
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Amazon FSx (Windows)

Before you begin, make sure that you have completed the following prerequisites.

In Amazon FSx (Windows), make sure you have:

- An Amazon FSx (Windows) account with read and mounting permissions.

- Noted your Amazon FSx authentication credentials for an Active Directory user account. This includes your Active Directory username and your Domain Name System (DNS) domain name. For example, *user@corp.example.com*.
- Copied your Amazon FSx file system ID.
- Used an Amazon VPC (AWS VPC) where your Amazon FSx resides.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Amazon FSx (Windows) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

You must also make sure you have configured your Amazon VPC instance with a NAT Gateway. For instructions on how to do this, see Step 1 of Connecting to a database in a VPC.

Connecting Amazon Q Business to Amazon FSx (Windows) using the console

The following procedure outlines how to connect Amazon Q Business to Amazon FSx (Windows) using the AWS Management Console.

Connecting Amazon Q to Amazon FSx (Windows)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.

4. Then, on the **Add data sources** page, from **Data sources**, add the **Amazon FSx (Windows)** data source to your Amazon Q application.
5. Then, on the **Amazon FSx (Windows)** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, for **Amazon FSx file system ID**—Select your file system ID or create a new directory.

   Only already created file system IDs are displayed and available to connect.
8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
9. **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name**—A name for your secret.

   b. For **User name**—Enter the username for Amazon FSx Active Directory account.

   c. For **Password**—Enter the password for the Amazon FSx Active Directory account.

   d. Choose **Save**.
10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

For more information, see VPC.

11. **Identity crawler** – Amazon Q crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.
12. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.
13. In **Sync scope**, enter the following information:

    a. **Regex patterns**—Add regular expression patterns to include or exclude certain content. You can add up to 100 patterns.

    b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

    c. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.
14. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

    For more details, see Sync mode.

15. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
16. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
17. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

18. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages,

including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Amazon FSx (Windows) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Amazon FSx JSON schema

The following is the Amazon FSx JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "fileSystemId": {
              "type": "string",
              "pattern": "fs-.*"
            },
            "fileSystemType": {
              "type": "string",
              "pattern": "WINDOWS"
            }
          },
          "required": ["fileSystemId", "fileSystemType"]
        }
      }
    },
```

```
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "All": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        }
      },
      "required": ["All"]
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
```

```
        "isCrawlAcl": {
          "type": "boolean"
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        },
        "exclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        }
      },
      "required": []
    },
    "enableIdentityCrawler": {
      "type": "boolean"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL"
      ]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "type" : {
      "type" : "string",
      "pattern": "FSX"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
```

```
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "secretArn",
    "enableIdentityCrawler",
    "additionalProperties",
    "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the endpoint for the data source.
`repositoryEndpointMetadata`	The endpoint information for the data source.
`fileSystemId`	The identifier of the Amazon FSx (Windows) file system. You can find your file system ID on the File Systems dashboard in the Amazon FSx (Windows) console.
`fileSystemType`	The type of Amazon FSx you use: Amazon FSx (Windows) file system.
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.
• `All`	A list of objects that map the attributes or field names of your Amazon FSx (Windows)

Configuration	Description
	pages and assets to Amazon Q index field names.
`additionalProperties`	Additional configuration options for your content in your data source.
`isCrawlAcl`	Specify `true` to crawl access control informati on from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
• `inclusionPatterns`	A list of regular expression patterns to include specific content from you Amazon FSx (Windows) data source. Content that match the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.

Configuration	Description
• `exclusionPatterns`	A list of regular expression patterns to exclude specific content from your Amazon FSx (Windows) data source. Content that match the patterns are excluded from the index. Content that doesn't match the patterns are included in the index. If content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.

Configuration	Description
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index
`type`	The type of data source. Specify `FSX` as your data source type.
`version`	The version of this template that's currently supported.

How Amazon Q Business connector crawls Amazon FSx (Windows) ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an Amazon FSx (Windows) data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from the directory service of the Amazon FSx instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

The group and user IDs are mapped as follows:

- `_group_ids`—Group IDs exist in Amazon FSx on files where there are set access permissions. They are mapped from the system group names in the directory service of Amazon FSx.

- `_user_id`—User IDs exist in Amazon FSx on files where there are set access permissions. They are mapped from the system user names in the directory service of Amazon FSx.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Amazon FSx (Windows) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Amazon FSx (Windows) connector supports the following entities and the associated reserved and custom attributes.

Amazon FSx (Windows) field name	Index field name	Description	Data type
creationTime	_created_at	Default	Date
lastModified	_last_updated_at	Default	Date
fileType	_file_type	Default	String
path	_source_uri	Default	String
author	_authors	Default	String list
size	fsx_size	Custom	String
lastAccessTime	_last_accessed_at	Custom	Date

IAM role for Amazon FSx (Windows) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.

- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
```

```
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
```

```
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting GitHub (Cloud) to Amazon Q Business

GitHub (Cloud) is a web-based hosting service for software development providing code storage and management services with version control. You can connect your GitHub (Cloud) instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- GitHub (Cloud) connector overview
- Prerequisites for connecting Amazon Q Business to GitHub (Cloud)
- Connecting Amazon Q Business to GitHub (Cloud) using the console
- Connecting Amazon Q Business to GitHub (Cloud) using APIs
- Connecting Amazon Q Business to GitHub (Cloud) using AWS CloudFormation
- How Amazon Q Business connector crawls GitHub Cloud ACLs
- GitHub (Cloud) data source connector field mappings
- IAM role for GitHub (Cloud) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.

- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

GitHub (Cloud) connector overview

The following table gives an overview of the Amazon Q Business GitHub (Cloud) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Personal token, OAuth token
	Authentication credentials	• GitHub (Cloud) token
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Entities**	Yes. The following entities are supported: • Repository • Repository Commit • Issue Document • Issue Comment • Issue Attachment • Pull Request Comment • Pull request Document • Pull Request Attachment See What is a document? for more details on what each connector crawls as a document.

Category	Feature	Support
	Field mappings	Yes. Supports default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include select repositories • Include content by specific entities. • Include specific branched by name • Include/exclude content by file name, file type, and file path
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to GitHub (Cloud)

Before you begin, make sure that you have completed the following prerequisites.

In GitHub (Cloud), make sure you have:

- Created a GitHub (Cloud) user with administrative permissions to the GitHub (Cloud) organization.
- Created a classic personal access token for authentication credentials. See GitHub (Cloud) documentation on creating a personal access token.
- **Recommended:** Created an OAuth token for authentication credentials. Use OAuth token for better API throttle limits and connector performance. See GitHub (Cloud) documentation on OAuth authorization.

  Then, added the following OAuth scopes:

  - `repo:status` – Grants read/write access to commit statuses in public and private repositories. This scope is only necessary to grant other users or services access to private repository commit statuses without granting access to the code.

- `repo_deployment` – Grants access to deployment statuses for public and private repositories. This scope is only necessary to grant other users or services access to deployment statuses, without granting access to the code.
- `public_repo` – Limits access to public repositories. That includes read/write access to code, commit statuses, repository projects, collaborators, and deployment statuses for public repositories and organizations. Also required for starring public repositories.
- `repo:invite` – Grants accept/decline abilities for invitations to collaborate on a repository. This scope is only necessary to grant other users or services access to invites without granting access to the code.
- `security_events` – Grants: read and write access to security events in the code scanning API. This scope is only necessary to grant other users or services access to security events without granting access to the code.
- `read:org` – Read-only access to organization membership, organization projects, and team membership.
- `user:email` – Grants read access to a user's email addresses. Required by Amazon Q Business to crawl ACLs.
- `user:follow` – Grants access to follow or unfollow other users. Required by Amazon Q Business to crawl ACLs.
- `read:user` – Grants access to read a user's profile data. Required by Amazon Q Business to crawl ACLs.
- `workflow` – Grants the ability to add and update GitHub (Cloud) Actions workflow files. Workflow files can be committed without this scope if the same file (with both the same path and contents) exists on another branch in the same repository.

  For more information, see Scopes for OAuth apps in GitHub (Cloud) Docs.

- Noted the GitHub (Cloud) host URL for the type of GitHub (Cloud) service that you use. For example, the host URL for GitHub (Cloud) Cloud could be *`https://api.github.com`*.
- Noted the name of your organization for GitHub (Cloud) the GitHub (Cloud) Enterprise account you want to connect to. You can find your organization name by logging into GitHub (Cloud) desktop and selecting **Your organizations** under your profile picture dropdown.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.

- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your GitHub (Cloud) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

> **Note**
>
> For more information on connecting GitHub (Cloud) to Amazon Q Business, see Connect the Amazon Q Business generative AI coding companion to your GitHub repositories with Amazon Q GitHub (Cloud) connector in the *AWS Machine Learning Blog*.

Connecting Amazon Q Business to GitHub (Cloud) using the console

The following procedure outlines how to connect Amazon Q Business to GitHub (Cloud) using the AWS Management Console.

Connecting Amazon Q to GitHub (Cloud)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **GitHub** data source to your Amazon Q application.
5. Then, on the **GitHub (Cloud)** data source page, enter the following information:
6. **Name and description**, do the following:

- For **Data source name** – Name your data source for easy tracking.

> **Note**
>
> You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. **Source** – Choose your GitHub (Cloud) source details.

   a. **GitHub (Cloud) source** – Choose GitHub (Cloud) Enterprise Cloud.

   b. **GitHub (Cloud) host URL** – Enter the GitHub (Cloud) host name with the protocol (http:// or https://). For example: *`https://api.github.com`*.

   c. **GitHub (Cloud) organization name** – You can find your organization name when you log in to GitHub (Cloud) desktop and go to **Your organizations** under your profile picture dropdown.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. **GitHub (Cloud) token** – Enter the access token you created in GitHub (Cloud).

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

12. In **Sync scope**, enter the following information:

    a. **Select repositories to crawl**—Select between crawling **All** repositories or **Select repositories**.

    If you choose **Select repositories**, add names for the repositories in **Name of repository** and, optionally, the name of any specific branches in **Name of branch**.

    b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

    c. **Additional configuration – *optional*** – Configure the following settings:

    - **Content types** – Select the file types you want to include. You can choose from the following options: **All**, **Files**, **Issues**, **Issue comments**, **Issue comment attachments**, **Pull request comment attachments**, **Pull requests**, and **Pull request comments**.
    - **Regex patterns** – Regular expression patterns to include or exclude certain files. You can add up to 100 patterns.

    d. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

13. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New or modified content sync** – Sync only new and modified documents.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

    For more details, see Sync mode.

14. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.

15. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.

16. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

    For more information, see Field mappings.

17. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to GitHub (Cloud) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- GitHub (Cloud) configuration properties
- GitHub (Cloud) JSON schema
- GitHub (Cloud) JSON schema example

GitHub (Cloud) configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-properties. • `hostUrl` • `type` • `organizationName`	Yes
`hostUrl`	The GitHub (Cloud) host URL. For example, if you use GitHub (Cloud) Enterprise Cloud: *https://api.github.com*.	`string`	Yes
`type`	The hosting method for your GitHub instance.	`string` The only allowed value is SAAS.	Yes
`organizationName`	You can find your organization name when you log in to GitHub (Cloud)	`string`	Yes

Configuration	Description	Type	Required
	desktop and go to **Your organizations** under your profile picture dropdown.		
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`array` This property has the following sub-properties: • `ghRepository` • `ghCommit` • `ghIssueDocument` • `ghIssueComment` • `ghIssueAttachment` • `ghPRDocument` • `ghPRComment` • `ghPRAttachment`	Yes

Configuration	Description	Type	Required
• ghRepository • ghCommit • ghIssueDocument • ghIssueComment • ghIssueAttachment • ghPRDocument • ghPRComment • ghPRAttachment	A list of objects that map the attributes or field names of your GitHub (Cloud) pages and assets to Amazon Q index field names.	object These properties have the following sub-properties. • indexFieldName • indexFieldType • dataSourceFieldName • dateFieldFormat	No
indexFieldName	The field name of your GitHub (Cloud) pages and assets.	string	Yes
indexFieldType	The field type of your GitHub (Cloud) pages and assets.	string The allowed values are STRING, STRING_LIST , and DATE.	Yes
dataSourceFieldName	The data source field name of your GitHub (Cloud) pages and assets.	string	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The date format of your GitHub (Cloud) pages and assets.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
`additionalProperties`	Additional configuration options for your content in your data source.	`object` This property has the following sub-properties. • `isCrawlAcl` • `crawlRepository` • `crawlRepositoryDocuments` • `crawlIssue` • `crawlIssueComment` • `crawlIssueCommentAttachment` • `crawlPullRequest` • `crawlPullRequestComment` • `crawlPullRequestCommentAttachment` • `fieldForUserId` • `maxFileSizeInMegaBytes`	Yes

Configuration	Description	Type	Required
		• `repositoryFilter` • `inclusionFolderNamePatterns` • `inclusionFileTypePatterns` • `inclusionFileNamePatterns` • `exclusionFolderNamePatterns` • `exclusionFileTypePatterns` • `exclusionFileNamePatterns`	
`isCrawlAcl`	Specify `true` to crawl access control information from documents.	`boolean`	No

Configuration	Description	Type	Required
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string` The allowed values are numbers between greater than 0 and less than or equal to 50.	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No
repositoryFilter	A list of names of the specific repositories and branch names you want to index.	`object` This property has the following sub-properties: `repositoryName` and `branchNameList` .	No
`repositoryName`	The list of repository names that you want to index.	`string`	No
`branchNameList`	The list of branch names that you want to index.	`array (string)`	No

Configuration	Description	Type	Required
`crawlRepository`	Specify `true` to crawl repositories.	`boolean`	No
`crawlRepositoryDocuments`	Specify `true` to crawl repository documents.	`boolean`	No
`crawlIssue`	Specify `true` to crawl issues.	`boolean`	No
`crawlIssueComment`	Specify `true` to crawl issue comments.	`boolean`	No
`crawlIssueCommentAttachment`	Specify `true` to crawl issue comment attachments.	`boolean`	No
`crawlPullRequest`	Specify `true` to crawl pull requests.	`boolean`	No
`crawlPullRequestComment`	Specify `true` to crawl pull request comments.	`boolean`	No
`crawlPullRequestCommentAttachment`	Specify `true` to crawl pull request comment attachments.	`boolean`	No

Configuration	Description	Type	Required
• `inclusionFolderNamePatterns` • `inclusionFileTypePatterns` • `inclusionFileNamePatterns`	A list of regular expression patterns to include specific content in your GitHub (Cloud) data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array (string)`	No

Configuration	Description	Type	Required
• `exclusionFolderNamePatterns` • `exclusionFileTypePatterns` • `exclusionFileNamePatterns`	A list of regular expression patterns to exclude specific content in your GitHub (Cloud) data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array (string)`	No
`type`	The type of data source. Specify `GITHUB` as your data source type.	`string`	Yes
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/ principal information on users and groups with access to specific documents.	`boolean`	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required

`secretArn`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your GitHub (Cloud).	`string`
		
		The secret must contain a JSON structure with the following keys:
		
		`{ "personal Token": " token" }`
			No

`version`	The version of this template that's currently supported.	`string`	No

GitHub (Cloud) JSON schema

The following is the GitHub (Cloud) JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "pattern": "GITHUB"
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
```

```
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "type": {
              "type": "string"
            },
            "hostUrl": {
              "type": "string",
              "pattern": "https://.*"
            },
            "organizationName": {
              "type": "string"
            }
          },
          "required": ["type", "hostUrl", "organizationName"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "ghRepository": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "ghCommit": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
```

```
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "ghIssueDocument": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
```

```
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "ghIssueComment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "ghIssueAttachment": {
        "type": "object",
```

```
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "ghPRDocument": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
```

```
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "ghPRComment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
```

```
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "ghPRAttachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
```

```
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "isCrawlAcl": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "fieldForUserId": {
        "type": "string"
      },
      "crawlRepository": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlRepositoryDocuments": {
        "anyOf": [
          {
            "type": "boolean"
          },
```

```
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlIssue": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlIssueComment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlIssueCommentAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlPullRequest": {
          "anyOf": [
            {
              "type": "boolean"
            },
```

```
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlPullRequestComment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlPullRequestCommentAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "repositoryFilter": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "repositoryName": {
                  "type": "string"
                },
                "branchNameList": {
                  "type": "array",
                  "items": {
                    "type": "string"
                  }
                }
              }
```

```
            }
          ]
        },
        "inclusionFolderNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFolderNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
```

```
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "syncMode",
    "enableIdentityCrawler",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

GitHub (Cloud) JSON schema example

The following is the GitHub (Cloud) JSON schema example:

```
{
  "type": "GITHUB",
  "syncMode": "FULL_CRAWL",
  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-github-secret",
  "enableIdentityCrawler": "true",
  "sslCertificatePath": {
    "bucket": "my-github-bucket",
    "key": "certificates/my-cert.pem"
```

```
  },
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "type": "GitHub",
      "hostUrl": "https://api.github.com",
      "organizationName": "my-org"
    }
  },
  "repositoryConfigurations": {
    "ghRepository": {
      "fieldMappings": [
        {
          "indexFieldName": "repo_name",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "name",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "ghCommit": {
      "fieldMappings": [
        {
          "indexFieldName": "commit_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    }
  },
  "additionalProperties": {
    "isCrawlAcl": "true",
    "maxFileSizeInMegaBytes": "50",
    "crawlRepository": "true",
    "crawlIssue": "true",
    "repositoryFilter": [
      {
        "repositoryName": "my-repo",
        "branchNameList": ["main", "develop"]
      }
    ],
    "inclusionFileTypePatterns": ["*.md", "*.txt"],
    "exclusionFileNamePatterns": ["*draft*"],
    "enableDeletionProtection": "false",
```

```
    "deletionProtectionThreshold": "15"
  },
  "version": "1.0.0"
}
```

Connecting Amazon Q Business to GitHub (Cloud) using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- GitHub (Cloud) configuration properties
- GitHub (Cloud) JSON schema for using the configuration property with AWS CloudFormation
- GitHub (Cloud) YAML schema for using the configuration property with AWS CloudFormation

GitHub (Cloud) configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object`	Yes

Configuration	Description	Type	Required
		This property has the following sub-properties. • `hostUrl` • `type` • `organizationName`	
`hostUrl`	The GitHub (Cloud) host URL. For example, if you use GitHub (Cloud) Enterprise Cloud: *https://api.github.com*.	`string`	Yes
`type`	The hosting method for your GitHub instance.	`string` The only allowed value is SAAS.	Yes
`organizationName`	You can find your organization name when you log in to GitHub (Cloud) desktop and go to **Your organizations** under your profile picture dropdown.	`string`	Yes

Configuration	Description	Type	Required
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`array` This property has the following sub-properties: • `ghRepository` • `ghCommit` • `ghIssueDocument` • `ghIssueComment` • `ghIssueAttachment` • `ghPRDocument` • `ghPRComment` • `ghPRAttachment`	Yes
• `ghRepository` • `ghCommit` • `ghIssueDocument` • `ghIssueComment` • `ghIssueAttachment` • `ghPRDocument` • `ghPRComment` • `ghPRAttachment`	A list of objects that map the attributes or field names of your GitHub (Cloud) pages and assets to Amazon Q index field names.	`object` These properties have the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName` • `dateFieldFormat`	No

Configuration	Description	Type	Required
`indexFieldName`	The field name of your GitHub (Cloud) pages and assets.	`string`	Yes
`indexFieldType`	The field type of your GitHub (Cloud) pages and assets.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes
`dataSourceFieldName`	The data source field name of your GitHub (Cloud) pages and assets.	`string`	Yes
`dateFieldFormat`	The date format of your GitHub (Cloud) pages and assets.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
`additionalProperties`	Additional configuration options for your content in your data source.	`object` This property has the following sub-properties. • `isCrawlAcl` • `crawlRepository` • `crawlRepositoryDocuments` • `crawlIssue` • `crawlIssueComment` • `crawlIssueCommentAttachment` • `crawlPullRequest` • `crawlPullRequestComment` • `crawlPullRequestCommentAttachment` • `fieldForUserId` • `maxFileSizeInMegaBytes`	Yes

Configuration	Description	Type	Required
		• `repositoryFilter` • `inclusionFolderNamePatterns` • `inclusionFileTypePatterns` • `inclusionFileNamePatterns` • `exclusionFolderNamePatterns` • `exclusionFileTypePatterns` • `exclusionFileNamePatterns`	
`isCrawlAcl`	Specify `true` to crawl access control information from documents.	`boolean`	No

Configuration	Description	Type	Required
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string` The allowed values are numbers between greater than 0 and less than or equal to 50.	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No
repositoryFilter	A list of names of the specific repositories and branch names you want to index.	`object` This property has the following sub-properties: `repositoryName` and `branchNameList` .	No
`repositoryName`	The list of repository names that you want to index.	`string`	No
`branchNameList`	The list of branch names that you want to index.	`array (string)`	No

Configuration	Description	Type	Required
crawlRepository	Specify true to crawl repositories.	boolean	No
crawlRepositoryDocuments	Specify true to crawl repository documents.	boolean	No
crawlIssue	Specify true to crawl issues.	boolean	No
crawlIssueComment	Specify true to crawl issue comments.	boolean	No
crawlIssueCommentAttachment	Specify true to crawl issue comment attachments.	boolean	No
crawlPullRequest	Specify true to crawl pull requests.	boolean	No
crawlPullRequestComment	Specify true to crawl pull request comments.	boolean	No
crawlPullRequestCommentAttachment	Specify true to crawl pull request comment attachments.	boolean	No

Configuration	Description	Type	Required
• `inclusionFolderNamePatterns` • `inclusionFileTypePatterns` • `inclusionFileNamePatterns`	A list of regular expression patterns to include specific content in your GitHub (Cloud) data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array (string)`	No

Configuration	Description	Type	Required
• `exclusionFolderNamePatterns` • `exclusionFileTypePatterns` • `exclusionFileNamePatterns`	A list of regular expression patterns to exclude specific content in your GitHub (Cloud) data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array (string)`	No
`type`	The type of data source. Specify `GITHUB` as your data source type.	`string`	Yes
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/ principal information on users and groups with access to specific documents.	`boolean`	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required

`secretArn`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your GitHub (Cloud).	`string`
		
		The secret must contain a JSON structure with the following keys:
		
		`{ "personal Token": " token" }`
			No

`version`	The version of this template that's currently supported.	`string`	No

GitHub (Cloud) JSON schema for using the configuration property with AWS CloudFormation

The following is the GitHub (Cloud) JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- GitHub (Cloud) JSON schema for using the configuration property with AWS CloudFormation
- GitHub (Cloud) JSON schema example for using the configuration property with AWS CloudFormation

GitHub (Cloud) JSON schema for using the configuration property with AWS CloudFormation

The following is the GitHub (Cloud) JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
```

```
      "pattern": "GITHUB"
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "type": {
              "type": "string"
            },
            "hostUrl": {
              "type": "string",
              "pattern": "https://.*"
            },
            "organizationName": {
              "type": "string"
            }
          },
          "required": ["type", "hostUrl", "organizationName"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
```

```
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "ghRepository": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "ghCommit": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
```

```
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "ghIssueDocument": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
```

```
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "ghIssueComment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
```

```
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "ghIssueAttachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
```

```
          "required": ["fieldMappings"]
        },
        "ghPRDocument": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "ghPRComment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
```

```
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "ghPRAttachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
```

```
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "isCrawlAcl": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "fieldForUserId": {
        "type": "string"
      },
      "crawlRepository": {
        "anyOf": [
          {
```

```
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlRepositoryDocuments": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlIssue": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlIssueComment": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlIssueCommentAttachment": {
        "anyOf": [
          {
```

```
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlPullRequest": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlPullRequestComment": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlPullRequestCommentAttachment": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "repositoryFilter": {
        "type": "array",
        "items": [
```

```
            {
              "type": "object",
              "properties": {
                "repositoryName": {
                  "type": "string"
                },
                "branchNameList": {
                  "type": "array",
                  "items": {
                    "type": "string"
                  }
                }
              }
            }
          ]
        },
        "inclusionFolderNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFolderNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
```

```
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "syncMode",
    "enableIdentityCrawler",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
```

```
}
```

GitHub (Cloud) JSON schema example for using the configuration property with AWS CloudFormation

The following is the GitHub (Cloud) JSON schema example for the configuration property for CloudFormation

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation GITHUB Data Source Template",
  "Resources": {
    "DataSourceGitHub": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MyGitHubDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "GITHUB",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-github-
secret",
          "enableIdentityCrawler": "true",
          "sslCertificatePath": {
            "bucket": "my-github-bucket",
            "key": "certificates/my-cert.pem"
          },
          "connectionConfiguration": {
            "repositoryEndpointMetadata": {
              "type": "GitHub",
              "hostUrl": "https://api.github.com",
              "organizationName": "my-org"
            }
          },
          "repositoryConfigurations": {
            "ghRepository": {
              "fieldMappings": [
                {
                  "indexFieldName": "repo_name",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "name",
```

```
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          },
          "ghCommit": {
            "fieldMappings": [
              {
                "indexFieldName": "commit_id",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          }
        },
        "additionalProperties": {
          "isCrawlAcl": "true",
          "maxFileSizeInMegaBytes": "50",
          "crawlRepository": "true",
          "crawlIssue": "true",
          "repositoryFilter": [
            {
              "repositoryName": "my-repo",
              "branchNameList": ["main", "develop"]
            }
          ],
          "inclusionFileTypePatterns": ["*.md", "*.txt"],
          "exclusionFileNamePatterns": ["*draft*"],
          "enableDeletionProtection": "false",
          "deletionProtectionThreshold": "15"
        }
      }
    }
  }
}
```

GitHub (Cloud) YAML schema for using the configuration property with AWS CloudFormation

The following is the GitHub (Cloud) YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- GitHub (Cloud) YAML schema for using the configuration property with AWS CloudFormation
- GitHub (Cloud) YAML schema example for using the configuration property with AWS CloudFormation

GitHub (Cloud) YAML schema for using the configuration property with AWS CloudFormation

The following is the GitHub (Cloud) YAML schema for the configuration property for CloudFormation.

```
type: object
properties:
  type:
    type: string
    pattern: GITHUB
  syncMode:
    type: string
    enum:
      - FULL_CRAWL
      - FORCED_FULL_CRAWL
      - CHANGE_LOG
  secretArn:
    type: string
    minLength: 20
    maxLength: 2048
  enableIdentityCrawler:
    anyOf:
      - type: boolean
      - type: string
        enum:
          - true
          - false
  connectionConfiguration:
    type: object
    properties:
      repositoryEndpointMetadata:
        type: object
        properties:
          type:
            type: string
          hostUrl:
            type: string
            pattern: "https://.*"
```

```
        organizationName:
          type: string
      required:
        - type
        - hostUrl
        - organizationName
  required:
    - repositoryEndpointMetadata
repositoryConfigurations:
  type: object
  properties:
    ghRepository:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    ghCommit:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
```

```
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    ghIssueDocument:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
```

```
              - indexFieldType
              - dataSourceFieldName
        required:
          - fieldMappings
      ghIssueComment:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      ghIssueAttachment:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
```

```
                - STRING
                - STRING_LIST
                - DATE
            dataSourceFieldName:
              type: string
            dateFieldFormat:
              type: string
              pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
          required:
            - indexFieldName
            - indexFieldType
            - dataSourceFieldName
      required:
        - fieldMappings
    ghPRDocument:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    ghPRComment:
      type: object
      properties:
```

```
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      ghPRAttachment:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
```

```
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
  additionalProperties:
    type: object
    properties:
      isCrawlAcl:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      maxFileSizeInMegaBytes:
        type: string
      fieldForUserId:
        type: string
      crawlRepository:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlRepositoryDocuments:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlIssue:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlIssueComment:
        anyOf:
```

```
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlIssueCommentAttachment:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlPullRequest:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlPullRequestComment:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlPullRequestCommentAttachment:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      repositoryFilter:
        type: array
        items:
          type: object
          properties:
            repositoryName:
              type: string
            branchNameList:
              type: array
              items:
                type: string
```

```
      inclusionFolderNamePatterns:
        type: array
        items:
          type: string
      inclusionFileTypePatterns:
        type: array
        items:
          type: string
      inclusionFileNamePatterns:
        type: array
        items:
          type: string
      exclusionFolderNamePatterns:
        type: array
        items:
          type: string
      exclusionFileTypePatterns:
        type: array
        items:
          type: string
      exclusionFileNamePatterns:
        type: array
        items:
          type: string
      enableDeletionProtection:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
        default: false
      deletionProtectionThreshold:
        type: string
        default: "15"
    required: []
  version:
    type: string
    anyOf:
      - pattern: 1.0.0
required:
  - syncMode
  - enableIdentityCrawler
  - connectionConfiguration
```

```
  - repositoryConfigurations
  - additionalProperties
```

GitHub (Cloud) YAML schema example for using the configuration property with AWS CloudFormation

The following is the GitHub (Cloud) YAML example for the Configuration property for CloudFormation:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: CloudFormation GITHUB Data Source Template
Resources:
  DataSourceGitHub:
    Type: AWS::QBusiness::DataSource
    Properties:
      ApplicationId: app12345-1234-1234-1234-123456789012
      IndexId: indx1234-1234-1234-1234-123456789012
      DisplayName: MyGitHubDataSource
      RoleArn: arn:aws:iam::123456789012:role/qbusiness-data-source-role
      Configuration:
        type: GITHUB
        syncMode: FULL_CRAWL
        secretArn: arn:aws:secretsmanager:us-west-2:123456789012:secret:my-github-
secret
        enableIdentityCrawler: "true"
        sslCertificatePath:
          bucket: my-github-bucket
          key: certificates/my-cert.pem
        connectionConfiguration:
          repositoryEndpointMetadata:
            type: GitHub
            hostUrl: https://api.github.com
            organizationName: my-org
        repositoryConfigurations:
          ghRepository:
            fieldMappings:
              - indexFieldName: repo_name
                indexFieldType: STRING
                dataSourceFieldName: name
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
          ghCommit:
            fieldMappings:
              - indexFieldName: commit_id
```

```
            indexFieldType: STRING
            dataSourceFieldName: id
            dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
        additionalProperties:
          isCrawlAcl: "true"
          maxFileSizeInMegaBytes: "50"
          crawlRepository: "true"
          crawlIssue: "true"
          repositoryFilter:
            - repositoryName: my-repo
              branchNameList:
                - main
                - develop
          inclusionFileTypePatterns:
            - "*.md"
            - "*.txt"
          exclusionFileNamePatterns:
            - "*draft*"
          enableDeletionProtection: "false"
          deletionProtectionThreshold: "15"
```

How Amazon Q Business connector crawls GitHub Cloud ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an GitHub Cloud data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your GitHub instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

GitHub Cloud's structure consists of repositories, teams, and projects. When you connect a GitHub Cloud data source to Amazon Q Business, it crawls GitHub Cloud repositories as defnied by your configuration, but it does not support teams or projects, meaning data related to team structures, internal communications, and project management is not retrieved. The child entities of repositories like Issues, Pull Requests, Files, and Comments are crawled.

When you connect an GitHub Cloud data source to Amazon Q Business, Amazon Q Business makes a copy of these resources and creates an index that can be used to respond to user prompts

and queries. Additionally, Amazon Q crawls ACL information attached to a document (user and group information) from your GitHub Cloud instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

Roles/permissions: GitHub Cloud has three roles:

- >Members - Default. Users with configurable repository and project permissions
- Owners - Users with full administrative control. There should be at least two for continuity.
- Outside Collaborators - Users who have restricted access to private repositories with managed permissions

The GitHub Cloud connector translates these roles into Amazon Q Business compatible ACLs, supporting View (Read), Edit, and Delete permissions. Since the lowest permission level is Read, more granular permissions beyond this do not impact data synchronization.

Identity Crawling: The connector supports both individual user and group synchronization. For Users, it maps repository-specific members and outside collaborators based on usernames, enforcing assigned GitHub Cloud permissions in Amazon Q. For Groups, it treats each repository as a group and members as organization group members. The connector retrieves ACL information for shared users based on repository name.

Permission Inheritance: There are three types of repositories:

- Public - Accessible to everyone; repositories inherit permissions from the organization.
- Private - Limited to the owner and explicitly granted collaborators. Does not inherit permissions from a parent. However, child entities such as Issues, Pull Requests, Files, and Comments inherit permissions from their parent repositories. When specific ACLs are definted, they replace the parent ACL.
- Internal - Accessible to all organization members but not to external users; repositories inherits permission from the organization

Change Management: Change Log Mode captures and logs any updates to access control lists (ACLs). When a user is removed from a private repository or deactivated, they are automatically excluded from the access list, and these changes are recorded in the change log. Change Log Mode enables incremental updates by indexing only newly added, updated, or deleted content since the last crawl, preventing unnecessary re-indexing. Any modifications to user access or permissions are also captured, ensuring accurate and up-to-date indexing of GitHub Cloud content.

Failure handling: The connector implements a fail-close approach, meaning that if there are permission-related issues or API failures, the document is skipped from ingestion rather than being made publicly accessible.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

GitHub (Cloud) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application environment and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q GitHub (Cloud) connector supports the following entities and the associated reserved and custom attributes.

> **Important**
>
> If you map any GitHub (Cloud) field to Amazon Q document title and document body fields, Amazon Q will generate responses from data in the document title and body.

> **Note**
>
> You can map any GitHub (Cloud) field to the document title or document body Amazon Q reserved/default index fields.

Supported entities and field mappings

- Repository
- Repository Commit
- Issue Document
- Issue Comment
- Issue Attachment
- Pull Request Comment
- Pull Request Document
- Pull Request Attachment

Repository

GitHub (Cloud) field name	Index field name	Description	Data type
Description	_document_body	Default	String
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String

GitHub (Cloud) field name	Index field name	Description	Data type
category	_category	Default	String
owner	_authors	Default	String list
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date

Repository Commit

GitHub (Cloud) field name	Index field name	Description	Data type
Description	_document_body	Default	String
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String
fileType	_file_type	Default	String
owner	_authors	Default	String list
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
fileName	gh_file_name	Default	String
fileSize	gh_size	Default	Long (numeric)

GitHub (Cloud) field name	Index field name	Description	Data type
branchName	gh_branch_name	Default	String

Issue Document

GitHub (Cloud) field name	Index field name	Description	Data type
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String
issueNumber	gh_issue_number	Custom	Long (numeric)
issueTitle	gh_issue_title	Custom	String
owner	_authors	Default	String list
fileType	_file_type	Default	String
issueSourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
issueFileName	gh_file_name	Custom	String
issueState	gh_issue_state	Custom	String
issueLabel	gh_issue_labels	Default	String list
issueAssignee	gh_issue_assignee	Default	String list

Issue Comment

GitHub (Cloud) field name	Index field name	Description	Data type
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String
issueNumber	gh_issue_number	Custom	Long (numeric)
issueTitle	gh_issue_title	Custom	String
owner	_authors	Default	String list
issueSourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
issueState	gh_issue_state	Custom	String
issueLabel	gh_issue_labels	Default	String list
issueAssignee	gh_issue_assignee	Default	String list

Issue Attachment

GitHub (Cloud) field name	Index field name	Description	Data type
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String

GitHub (Cloud) field name	Index field name	Description	Data type
category	_category	Default	String
issueNumber	gh_issue_number	Custom	Long (numeric)
issueTitle	gh_issue_title	Custom	String
owner	_authors	Default	String list
issueSourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
issueFileName	gh_file_name	Custom	String
issueFileType	_file_type	Custom	String
issueState	gh_issue_state	Custom	String
issueLabel	gh_issue_labels	Default	String list
issueAssignee	gh_issue_assignee	Default	String list

Pull Request Comment

GitHub (Cloud) field name	Index field name	Description	Data type
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String
PRNumber	gh_pr_number	Custom	Long (numeric)

GitHub (Cloud) field name	Index field name	Description	Data type
PRTitle	gh_pr_title	Custom	String
owner	_authors	Default	String list
PRSourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
PRState	gh_pr_state	Custom	String
PRLabel	gh_pr_labels	Default	String list
PRAssignee	gh_pr_assignee	Default	String list

Pull Request Document

GitHub (Cloud) field name	Index field name	Description	Data type
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String
PRNumber	gh_number	Custom	Long (numeric)
PRTitle	gh_pr_title	Custom	String
owner	_authors	Default	String list
PRSourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date

GitHub (Cloud) field name	Index field name	Description	Data type
updatedAt	_last_updated_at	Default	Date
PRFileName	gh_file_name	Custom	String
PRFileType	_file_type	Custom	String
PRState	gh_pr_state	Custom	String
PRLabel	gh_pr_labels	Default	String list
PRAssignee	gh_pr_assignee	Default	String list

Pull Request Attachment

GitHub (Cloud) field name	Index field name	Description	Data type
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String
PRNumber	gh_number	Custom	Long (numeric)
PRTitle	gh_pr_title	Custom	String
owner	_authors	Default	String list
PRSourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
PRFileName	gh_file_name	Custom	String

GitHub (Cloud) field name	Index field name	Description	Data type
PRFileType	_file_type	Custom	String
PRState	gh_pr_state	Custom	String
PRLabel	gh_pr_labels	Default	String list
PRAssignee	gh_pr_assignee	Default	String list

IAM role for GitHub (Cloud) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
```

```
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
```

```
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
```

```
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting GitHub (Server) to Amazon Q Business

GitHub (Server) is a web-based hosting service for software development providing code storage and management services with version control. You can connect your GitHub (Server) instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- GitHub (Server) connector overview
- Prerequisites for connecting Amazon Q Business to GitHub (Server)
- Connecting Amazon Q Business to GitHub (Server) using the console
- Connecting Amazon Q Business to GitHub (Server) using APIs
- Connecting Amazon Q Business to GitHub (Server) using AWS CloudFormation

- How Amazon Q Business connector crawls GitHub Server ACLs
- GitHub (Server) data source connector field mappings
- IAM role for GitHub (Server) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

GitHub (Server) connector overview

The following table gives an overview of the Amazon Q Business GitHub (Server) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	OAuth token, Personal token
	Authentication credentials	• GitHub token
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Entities**	Yes. The following entities are supported: • Repository • Repository Commit • Issue Document

Category	Feature	Support
		• Issue Comment • Issue Attachment • Pull Request Comment • Pull request Document • Pull Request Attachment See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include select repositories • Include content by specific entities. • Include specific branched by name • Include/exclude content by file name, file type, and file path
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to GitHub (Server)

Before you begin, make sure that you have completed the following prerequisites.

In GitHub (Server), make sure you have:

- Created a GitHub (Server) user with administrative permissions to the GitHub (Server) organization.
- Created a classic personal access token for authentication credentials. See GitHub documentation on creating a personal access token.

- **Recommended:**Created an OAuth token for authentication credentials. Use OAuth token for better API throttle limits and connector performance. See GitHub documentation on OAuth authorization.

  Then, added the following OAuth scopes:

  - `repo:status` – Grants read/write access to commit statuses in public and private repositories. This scope is only necessary to grant other users or services access to private repository commit statuses without granting access to the code.
  - `repo_deployment` – Grants access to deployment statuses for public and private repositories. This scope is only necessary to grant other users or services access to deployment statuses, without granting access to the code.
  - `public_repo` – Limits access to public repositories. That includes read/write access to code, commit statuses, repository projects, collaborators, and deployment statuses for public repositories and organizations. Also required for starring public repositories.
  - `repo:invite` – Grants accept/decline abilities for invitations to collaborate on a repository. This scope is only necessary to grant other users or services access to invites without granting access to the code.
  - `security_events` – Grants: read and write access to security events in the code scanning API. This scope is only necessary to grant other users or services access to security events without granting access to the code.
  - `read:org` – Read-only access to organization membership, organization projects, and team membership.
  - `user:email` – Grants read access to a user's email addresses. Required by Amazon Q Business to crawl ACLs.
  - `user:follow` – Grants access to follow or unfollow other users. Required by Amazon Q Business to crawl ACLs.
  - `read:user` – Grants access to read a user's profile data. Required by Amazon Q Business to crawl ACLs.
  - `workflow` – Grants the ability to add and update GitHub (Server) Actions workflow files. Workflow files can be committed without this scope if the same file (with both the same path and contents) exists on another branch in the same repository.

  For more information, see Scopes for OAuth apps in GitHub (Server) Docs.

- Noted the GitHub (Server) host URL for the type of GitHub (Server) service that you use. For example, the host URL for GitHub (Server) Server could be *`https://on-prem-host-url/api/v3/`*.
- Noted the name of your organization for GitHub (Server) the GitHub Enterprise account you want to connect to. You can find your organization name by logging into GitHub (Server) desktop and selecting **Your organizations** under your profile picture dropdown.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your GitHub (Server) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to GitHub (Server) using the console

The following procedure outlines how to connect Amazon Q Business to GitHub (Server) using the AWS Management Console.

Connecting Amazon Q to GitHub (Server)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **GitHub** data source to your Amazon Q application.

5. Then, on the **GitHub (Server)** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. **Source** – Choose your GitHub (Server) source details.

   a. **GitHub (Server) source** – Choose GitHub (Server) Enterprise Cloud.

   b. **GitHub (Server) host URL** – Enter the GitHub (Server) host name with the protocol (http:// or https://). For example: *`https://on-prem-host-url/api/v3/`*.

   c. **GitHub (Server) organization name** – You can find your organization name when you log in to GitHub (Server) desktop and go to **Your organizations** under your profile picture dropdown.

   d. **SSL certificate location**— Enter the path to the SSL certificate stored in an Amazon S3 bucket. You use this to connect to Github (Server) with a secure SSL connection.
8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
9. **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. **GitHub (Server) token** – Enter the access token you created in GitHub.
10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

12. In **Sync scope**, enter the following information:

a. **Select repositories to crawl**—Select between crawling **All** repositories or **Select repositories**.

If you choose **Select repositories**, add names for the repositories in **Name of repository** and, optionally, the name of any specific branches in **Name of branch**.

b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

c. **Additional configuration – *optional*** – Configure the following settings:

- **Content types** – Select the file types you want to include. You can choose from the following options: **All**, **Files**, **Issues**, **Issue comments**, **Issue comment attachments**, **Pull request comment attachments**, **Pull requests**, and **Pull request comments**.
- **Regex patterns** – Regular expression patterns to include or exclude certain files. You can add up to 100 patterns.

d. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete

phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

13. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New or modified content sync** – Sync only new and modified documents.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

    For more details, see Sync mode.

14. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
15. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
16. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

    For more information, see Field mappings.

17. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to GitHub (Server) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- GitHub (Cloud) configuration properties
- GitHub (Server) JSON schema
- GitHub (Server) JSON schema example

GitHub (Cloud) configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-properties. • `hostUrl` • `type` • `organizationName`	Yes
`hostUrl`	The GitHub (Cloud) host URL. For example, if you use GitHub (Cloud) Enterprise Server: *https://on-prem-host-url/api/v3/*.	`string`	Yes
`type`	The hosting method for your GitHub instance.	`string` The only allowed value is `ON_PREMISE` .	Yes
`organizationName`	You can find your organization name when you log in	`string`	Yes

Configuration	Description	Type	Required
	to GitHub (Cloud) desktop and go to **Your organizations** under your profile picture dropdown.		
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties: • `ghRepository` • `ghCommit` • `ghIssueDocument` • `ghIssueComment` • `ghIssueAttachment` • `ghPRDocument` • `ghPRComment` • `ghPRAttachment`	Yes

Configuration	Description	Type	Required
• ghRepository • ghCommit • ghIssueDocument • ghIssueComment • ghIssueAttachment • ghPRDocument • ghPRComment • ghPRAttachment	A list of objects that map the attributes or field names of your GitHub pages and assets to Amazon Q index field names.	object These properties have the following sub-properties. • indexFieldName • indexFieldType • dataSourceFieldName • dateFieldFormat	No
indexFieldName	The field name of your GitHub (Cloud) pages and assets.	string	Yes
indexFieldType	The field type of your GitHub (Cloud) pages and assets.	string The allowed values are STRING, STRING_LIST , and DATE.	Yes
dataSourceFieldName	The data source field name of your GitHub (Cloud) pages and assets.	string	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The date format of your GitHub (Cloud) pages and assets.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties. • isCrawlAcl • crawlRepository • crawlRepositoryDocuments • crawlIssue • crawlIssueComment • crawlIssueCommentAttachment • crawlPullRequest • crawlPullRequestComment • crawlPullRequestCommentAttachment • fieldForUserId • maxFileSizeInMegaBytes	Yes

Configuration	Description	Type	Required
		• `repositoryFilter` • `inclusionFolderNamePatterns` • `inclusionFileTypePatterns` • `inclusionFileNamePatterns` • `exclusionFolderNamePatterns` • `exclusionFileTypePatterns` • `exclusionFileNamePatterns`	
`isCrawlAcl`	Specify `true` to crawl access control information from documents.	`boolean`	No

Configuration	Description	Type	Required
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string` The allowed values are numbers between greater than 0 and less than or equal to 50.	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No
repositoryFilter	A list of names of the specific repositories and branch names you want to index.	`object` This property has the following sub-properties: `repositoryName` and `branchNameList` .	No
`repositoryName`	The list of repository names that you want to index.	`string`	No
`branchNameList`	The list of branch names that you want to index.	`array (string)`	No

Configuration	Description	Type	Required
`crawlRepository`	Specify `true` to crawl repositories.	`boolean`	No
`crawlRepositoryDocuments`	Specify `true` to crawl repository documents.	`boolean`	No
`crawlIssue`	Specify `true` to crawl issues.	`boolean`	No
`crawlIssueComment`	Specify `true` to crawl issue comments.	`boolean`	No
`crawlIssueCommentAttachment`	Specify `true` to crawl issue comment attachments.	`boolean`	No
`crawlPullRequest`	Specify `true` to crawl pull requests.	`boolean`	No
`crawlPullRequestComment`	Specify `true` to crawl pull request comments.	`boolean`	No
`crawlPullRequestCommentAttachment`	Specify `true` to crawl pull request comment attachments.	`boolean`	No

Configuration	Description	Type	Required
• `inclusionFolderNamePatterns` • `inclusionFileTypePatterns` • `inclusionFileNamePatterns`	A list of regular expression patterns to include specific content in your GitHub data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array (string)`	No

Configuration	Description	Type	Required
• `exclusionFolderNamePatterns` • `exclusionFileTypePatterns` • `exclusionFileNamePatterns`	A list of regular expression patterns to exclude specific content in your GitHub data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array (string)`	No
`type`	The type of data source. Specify `GITHUB` as your data source type.	`string`	Yes
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/ principal information on users and groups with access to specific documents.	`boolean`	Yes

Configuration	Description	Type	Required
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	`string` You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required

`secretArn`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your GitHub (Cloud).	`string`
		
		The secret must contain a JSON structure with the following keys:
		
		`{ "personal Token": " token" }`
			No

`version`	The version of this template that's currently supported.	`string`	No

GitHub (Server) JSON schema

The following is the GitHub (Server) JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "pattern": "GITHUB"
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
```

```
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "sslCertificatePath": {
      "type": "object",
      "properties": {
        "bucket": {
          "type": "string",
          "pattern": "^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$",
          "minLength": 3,
          "maxLength": 63
        },
        "key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 10240
        }
      },
      "required": ["bucket", "key"]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "type": {
              "type": "string"
            },
            "hostUrl": {
              "type": "string",
              "pattern": "https://.*"
            },
            "organizationName": {
              "type": "string"
            }
          },
          "required": ["type", "hostUrl", "organizationName"]
```

```
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "ghRepository": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "ghCommit": {
          "type": "object",
```

```
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "ghIssueDocument": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
```

```
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "ghIssueComment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
```

```
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "ghIssueAttachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
```

```
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "ghPRDocument": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "ghPRComment": {
      "type": "object",
      "properties": {
```

```
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "ghPRAttachment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
```

```
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "isCrawlAcl": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "fieldForUserId": {
        "type": "string"
```

```
        },
        "crawlRepository": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlRepositoryDocuments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlIssue": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlIssueComment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
```

```
        },
        "crawlIssueCommentAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlPullRequest": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlPullRequestComment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlPullRequestCommentAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
```

```
        },
        "repositoryFilter": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "repositoryName": {
                  "type": "string"
                },
                "branchNameList": {
                  "type": "array",
                  "items": {
                    "type": "string"
                  }
                }
              }
            }
          ]
        },
        "inclusionFolderNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFolderNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
```

```
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "syncMode",
    "enableIdentityCrawler",
    "connectionConfiguration",
```

```
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

GitHub (Server) JSON schema example

The following is the GitHub (Server) JSON schema example:

```
{
  "type": "GITHUB",
  "syncMode": "FULL_CRAWL",
  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-github-secret",
  "enableIdentityCrawler": "true",
  "sslCertificatePath": {
    "bucket": "my-github-bucket",
    "key": "certificates/my-cert.pem"
  },
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "type": "GitHub",
      "hostUrl": "https://host.url.com",
      "organizationName": "my-org"
    }
  },
  "repositoryConfigurations": {
    "ghRepository": {
      "fieldMappings": [
        {
          "indexFieldName": "repo_name",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "name",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "ghCommit": {
      "fieldMappings": [
        {
          "indexFieldName": "commit_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
```

```
      ]
    }
  },
  "additionalProperties": {
    "isCrawlAcl": "true",
    "maxFileSizeInMegaBytes": "50",
    "crawlRepository": "true",
    "crawlIssue": "true",
    "repositoryFilter": [
      {
        "repositoryName": "my-repo",
        "branchNameList": ["main", "develop"]
      }
    ],
    "inclusionFileTypePatterns": ["*.md", "*.txt"],
    "exclusionFileNamePatterns": ["*draft*"],
    "enableDeletionProtection": "false",
    "deletionProtectionThreshold": "15"
  },
  "version": "1.0.0"
}
```

Connecting Amazon Q Business to GitHub (Server) using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- GitHub (Cloud) configuration properties
- GitHub (Server) JSON schema for using the configuration property with AWS CloudFormation
- GitHub (Server) YAML schema for using the configuration property with AWS CloudFormation

GitHub (Cloud) configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-properties. • `hostUrl` • `type` • `organizationName`	Yes
`hostUrl`	The GitHub (Cloud) host URL. For example, if you use GitHub (Cloud) Enterprise Server: *https://on-prem-host-url/api/v3/*.	`string`	Yes
`type`	The hosting method for your GitHub instance.	`string`	Yes

Configuration	Description	Type	Required
		The only allowed value is `ON_PREMISE` .	
`organizationName`	You can find your organization name when you log in to GitHub (Cloud) desktop and go to **Your organizations** under your profile picture dropdown.	`string`	Yes
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties: • `ghRepository` • `ghCommit` • `ghIssueDocument` • `ghIssueComment` • `ghIssueAttachment` • `ghPRDocument` • `ghPRComment` • `ghPRAttachment`	Yes

Configuration	Description	Type	Required
• ghRepository • ghCommit • ghIssueDocument • ghIssueComment • ghIssueAttachment • ghPRDocument • ghPRComment • ghPRAttachment	A list of objects that map the attributes or field names of your GitHub pages and assets to Amazon Q index field names.	object These properties have the following sub-properties. • indexFieldName • indexFieldType • dataSourceFieldName • dateFieldFormat	No
indexFieldName	The field name of your GitHub (Cloud) pages and assets.	string	Yes
indexFieldType	The field type of your GitHub (Cloud) pages and assets.	string The allowed values are STRING, STRING_LIST , and DATE.	Yes
dataSourceFieldName	The data source field name of your GitHub (Cloud) pages and assets.	string	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The date format of your GitHub (Cloud) pages and assets.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties. • isCrawlAcl • crawlRepository • crawlRepositoryDocuments • crawlIssue • crawlIssueComment • crawlIssueCommentAttachment • crawlPullRequest • crawlPullRequestComment • crawlPullRequestCommentAttachment • fieldForUserId • maxFileSizeInMegaBytes	Yes

Configuration	Description	Type	Required
		• repositoryFilter • inclusionFolderNamePatterns • inclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFolderNamePatterns • exclusionFileTypePatterns • exclusionFileNamePatterns	
isCrawlAcl	Specify true to crawl access control information from documents.	boolean	No

Configuration	Description	Type	Required
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string` The allowed values are numbers between greater than 0 and less than or equal to 50.	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No
repositoryFilter	A list of names of the specific repositories and branch names you want to index.	`object` This property has the following sub-properties: `repositoryName` and `branchNameList` .	No
`repositoryName`	The list of repository names that you want to index.	`string`	No
`branchNameList`	The list of branch names that you want to index.	`array (string)`	No

Configuration	Description	Type	Required
`crawlRepository`	Specify `true` to crawl repositories.	`boolean`	No
`crawlRepositoryDocuments`	Specify `true` to crawl repository documents.	`boolean`	No
`crawlIssue`	Specify `true` to crawl issues.	`boolean`	No
`crawlIssueComment`	Specify `true` to crawl issue comments.	`boolean`	No
`crawlIssueCommentAttachment`	Specify `true` to crawl issue comment attachments.	`boolean`	No
`crawlPullRequest`	Specify `true` to crawl pull requests.	`boolean`	No
`crawlPullRequestComment`	Specify `true` to crawl pull request comments.	`boolean`	No
`crawlPullRequestCommentAttachment`	Specify `true` to crawl pull request comment attachments.	`boolean`	No

Configuration	Description	Type	Required
• `inclusionFolderNamePatterns` • `inclusionFileTypePatterns` • `inclusionFileNamePatterns`	A list of regular expression patterns to include specific content in your GitHub data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array (string)`	No

Configuration	Description	Type	Required
• exclusionFolderNamePatterns • exclusionFileTypePatterns • exclusionFileNamePatterns	A list of regular expression patterns to exclude specific content in your GitHub data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	array (string)	No
type	The type of data source. Specify GITHUB as your data source type.	string	Yes
enableIdentityCrawler	Specify true to use the Amazon Q identity crawler to sync identity/ principal information on users and groups with access to specific documents.	boolean	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required

`secretArn`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your GitHub (Cloud).	`string`
		
		The secret must contain a JSON structure with the following keys:
		
		`{ "personalToken": " token" }`
			No

`version`	The version of this template that's currently supported.	`string`	No

GitHub (Server) JSON schema for using the configuration property with AWS CloudFormation

The following is the GitHub (Server) JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- GitHub (Server) JSON schema for using the configuration property with AWS CloudFormation
- GitHub (Server) JSON schema example for using the configuration property with AWS CloudFormation

GitHub (Server) JSON schema for using the configuration property with AWS CloudFormation

The following is the GitHub (Server) JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
```

```
      "pattern": "GITHUB"
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "sslCertificatePath": {
      "type": "object",
      "properties": {
        "bucket": {
          "type": "string",
          "pattern": "^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$",
          "minLength": 3,
          "maxLength": 63
        },
        "key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 10240
        }
      },
      "required": ["bucket", "key"]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
```

```
          "properties": {
            "type": {
              "type": "string"
            },
            "hostUrl": {
              "type": "string",
              "pattern": "https://.*"
            },
            "organizationName": {
              "type": "string"
            }
          },
          "required": ["type", "hostUrl", "organizationName"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "ghRepository": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
```

```
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "ghCommit": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
```

```
          "required": ["fieldMappings"]
        },
        "ghIssueDocument": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "ghIssueComment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
```

```
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "ghIssueAttachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
```

```
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "ghPRDocument": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
```

```
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "ghPRComment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
```

```
        },
        "ghPRAttachment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        }
      }
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "isCrawlAcl": {
          "anyOf": [
            {
```

```
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "fieldForUserId": {
        "type": "string"
      },
      "crawlRepository": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlRepositoryDocuments": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlIssue": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
```

```
            }
          ]
        },
        "crawlIssueComment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlIssueCommentAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlPullRequest": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlPullRequestComment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
```

```
            }
          ]
        },
        "crawlPullRequestCommentAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "repositoryFilter": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "repositoryName": {
                  "type": "string"
                },
                "branchNameList": {
                  "type": "array",
                  "items": {
                    "type": "string"
                  }
                }
              }
            }
          ]
        },
        "inclusionFolderNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
```

```
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFolderNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    },
```

```
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "syncMode",
    "enableIdentityCrawler",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

GitHub (Server) JSON schema example for using the configuration property with AWS CloudFormation

The following is the GitHub (Server) JSON schema example for the configuration property for CloudFormation

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation GITHUB Data Source Template",
  "Resources": {
    "DataSourceGitHub": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MyGitHubDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "GITHUB",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-github-
secret",
          "enableIdentityCrawler": "true",
          "sslCertificatePath": {
            "bucket": "my-github-bucket",
```

```
            "key": "certificates/my-cert.pem"
          },
          "connectionConfiguration": {
            "repositoryEndpointMetadata": {
              "type": "GitHub",
              "hostUrl": "https://host.url.com",
              "organizationName": "my-org"
            }
          },
          "repositoryConfigurations": {
            "ghRepository": {
              "fieldMappings": [
                {
                  "indexFieldName": "repo_name",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "name",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
            },
            "ghCommit": {
              "fieldMappings": [
                {
                  "indexFieldName": "commit_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
            }
          },
          "additionalProperties": {
            "isCrawlAcl": "true",
            "maxFileSizeInMegaBytes": "50",
            "crawlRepository": "true",
            "crawlIssue": "true",
            "repositoryFilter": [
              {
                "repositoryName": "my-repo",
                "branchNameList": ["main", "develop"]
              }
            ],
            "inclusionFileTypePatterns": ["*.md", "*.txt"],
            "exclusionFileNamePatterns": ["*draft*"],
```

```
            "enableDeletionProtection": "false",
            "deletionProtectionThreshold": "15"
          }
        }
      }
    }
  }
}
```

GitHub (Server) YAML schema for using the configuration property with AWS CloudFormation

The following is the GitHub (Server) YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- GitHub (Server) YAML schema for using the configuration property with AWS CloudFormation
- GitHub (Server) YAML schema example for using the configuration property with AWS CloudFormation

GitHub (Server) YAML schema for using the configuration property with AWS CloudFormation

The following is the GitHub (Server) YAML schema for the configuration property for CloudFormation.

```
type: object
properties:
  type:
    type: string
    pattern: GITHUB
  syncMode:
    type: string
    enum:
      - FULL_CRAWL
      - FORCED_FULL_CRAWL
      - CHANGE_LOG
  secretArn:
    type: string
    minLength: 20
    maxLength: 2048
  enableIdentityCrawler:
    anyOf:
```

```
      - type: boolean
      - type: string
        enum:
          - true
          - false
  sslCertificatePath:
    type: object
    properties:
      bucket:
        type: string
        pattern: "^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$"
        minLength: 3
        maxLength: 63
      key:
        type: string
        minLength: 1
        maxLength: 10240
    required:
      - bucket
      - key
  connectionConfiguration:
    type: object
    properties:
      repositoryEndpointMetadata:
        type: object
        properties:
          type:
            type: string
          hostUrl:
            type: string
            pattern: "https://.*"
          organizationName:
            type: string
        required:
          - type
          - hostUrl
          - organizationName
    required:
      - repositoryEndpointMetadata
  repositoryConfigurations:
    type: object
    properties:
      ghRepository:
        type: object
```

```
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
          required:
            - fieldMappings
      ghCommit:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
```

```
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    ghIssueDocument:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    ghIssueComment:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
```

```
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    ghIssueAttachment:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
```

```
      - fieldMappings
    ghPRDocument:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
          required:
            - indexFieldName
            - indexFieldType
            - dataSourceFieldName
      required:
        - fieldMappings
    ghPRComment:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
```

```
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    ghPRAttachment:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
additionalProperties:
  type: object
  properties:
    isCrawlAcl:
      anyOf:
        - type: boolean
```

```
          - type: string
            enum:
              - true
              - false
      maxFileSizeInMegaBytes:
        type: string
      fieldForUserId:
        type: string
      crawlRepository:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlRepositoryDocuments:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlIssue:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlIssueComment:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlIssueCommentAttachment:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlPullRequest:
```

```
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlPullRequestComment:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlPullRequestCommentAttachment:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      repositoryFilter:
        type: array
        items:
          type: object
          properties:
            repositoryName:
              type: string
            branchNameList:
              type: array
              items:
                type: string
      inclusionFolderNamePatterns:
        type: array
        items:
          type: string
      inclusionFileTypePatterns:
        type: array
        items:
          type: string
      inclusionFileNamePatterns:
        type: array
        items:
          type: string
      exclusionFolderNamePatterns:
```

```
        type: array
        items:
          type: string
      exclusionFileTypePatterns:
        type: array
        items:
          type: string
      exclusionFileNamePatterns:
        type: array
        items:
          type: string
      enableDeletionProtection:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
        default: false
      deletionProtectionThreshold:
        type: string
        default: "15"
    required: []
  version:
    type: string
    anyOf:
      - pattern: 1.0.0
required:
  - syncMode
  - enableIdentityCrawler
  - connectionConfiguration
  - repositoryConfigurations
  - additionalProperties
```

GitHub (Server) YAML schema example for using the configuration property with AWS CloudFormation

The following is the GitHub (Server) YAML example for the Configuration property for CloudFormation:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: CloudFormation GITHUB Data Source Template
Resources:
```

```
  DataSourceGitHub:
    Type: AWS::QBusiness::DataSource
    Properties:
      ApplicationId: app12345-1234-1234-1234-123456789012
      IndexId: indx1234-1234-1234-1234-123456789012
      DisplayName: MyGitHubDataSource
      RoleArn: arn:aws:iam::123456789012:role/qbusiness-data-source-role
      Configuration:
        type: GITHUB
        syncMode: FULL_CRAWL
        secretArn: arn:aws:secretsmanager:us-west-2:123456789012:secret:my-github-
secret
        enableIdentityCrawler: "true"
        sslCertificatePath:
          bucket: my-github-bucket
          key: certificates/my-cert.pem
        connectionConfiguration:
          repositoryEndpointMetadata:
            type: GitHub
            hostUrl: https://api.github.com
            organizationName: my-org
        repositoryConfigurations:
          ghRepository:
            fieldMappings:
              - indexFieldName: repo_name
                indexFieldType: STRING
                dataSourceFieldName: name
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
          ghCommit:
            fieldMappings:
              - indexFieldName: commit_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
        additionalProperties:
          isCrawlAcl: "true"
          maxFileSizeInMegaBytes: "50"
          crawlRepository: "true"
          crawlIssue: "true"
          repositoryFilter:
            - repositoryName: my-repo
              branchNameList:
                - main
                - develop
```

```
        inclusionFileTypePatterns:
          - "*.md"
          - "*.txt"
        exclusionFileNamePatterns:
          - "*draft*"
        enableDeletionProtection: "false"
        deletionProtectionThreshold: "15"
```

How Amazon Q Business connector crawls GitHub Server ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an GitHub Server data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your GitHub instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

GitHub Server's structure consists of repositories, teams, and projects. When you connect a GitHub Server data source to Amazon Q Business, it crawls GitHub Server repositories as defnied by your configuration, but it does not support teams or projects, meaning data related to team structures, internal communications, and project management is not retrieved. The child entities of repositories like Issues, Pull Requests, Files, and Comments are crawled.

When you connect an GitHub Server data source to Amazon Q Business, Amazon Q Business makes a copy of these resources and creates an index that can be used to respond to user prompts and queries. Additionally, Amazon Q crawls ACL information attached to a document (user and group information) from your GitHub Server instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

Roles/permissions: GitHub Server has three roles:

- >Members - Default. Users with configurable repository and project permissions
- Owners - Users with full administrative control. There should be at least two for continuity.
- Outside Collaborators - Users who have restricted access to private repositories with managed permissions

The GitHub Server connector translates these roles into Amazon Q Business compatible ACLs, supporting View (Read), Edit, and Delete permissions. Since the lowest permission level is Read, more granular permissions beyond this do not impact data synchronization.

Identity Crawling: The connector supports both individual user and group synchronization. For Users, it maps repository-specific members and outside collaborators based on usernames, enforcing assigned GitHub Server permissions in Amazon Q. For Groups, it treats each repository as a group and members as organization group members. The connector retrieves ACL information for shared users based on repository name.

Permission Inheritance: There are three types of repositories:

- Public - Accessible to everyone; repositories inherit permissions from the organization.
- Private - Limited to the owner and explicitly granted collaborators. Does not inherit permissions from a parent. However, child entities such as Issues, Pull Requests, Files, and Comments inherit permissions from their parent repositories. When specific ACLs are definted, they replace the parent ACL.
- Internal - Accessible to all organization members but not to external users; repositories inherits permission from the organization

Change Management: Change Log Mode captures and logs any updates to access control lists (ACLs). When a user is removed from a private repository or deactivated, they are automatically excluded from the access list, and these changes are recorded in the change log. Change Log Mode enables incremental updates by indexing only newly added, updated, or deleted content since the last crawl, preventing unnecessary re-indexing. Any modifications to user access or permissions are also captured, ensuring accurate and up-to-date indexing of GitHub Server content.

Failure handling: The connector implements a fail-close approach, meaning that if there are permission-related issues or API failures, the document is skipped from ingestion rather than being made publicly accessible.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

GitHub (Server) data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application environment and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q GitHub connector supports the following entities and the associated reserved and custom attributes.

> **Important**
>
> If you map any GitHub (Server) field to Amazon Q document title and document body fields, Amazon Q will generate responses from data in the document title and body.

Note

You can map any GitHub field to the document title or document body Amazon Q reserved/default index fields.

Supported entities and field mappings

- Repository
- Repository Commit
- Issue Document
- Issue Comment
- Issue Attachment
- Pull Request Comment
- Pull Request Document
- Pull Request Attachment

Repository

GitHub field name	Index field name	Description	Data type
Description	_document_body	Default	String
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String
owner	_authors	Default	String list
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date

Repository Commit

GitHub field name	Index field name	Description	Data type
Description	_document_body	Default	String
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String
fileType	_file_type	Default	String
owner	_authors	Default	String list
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
fileName	gh_file_name	Default	String
fileSize	gh_size	Default	Long (numeric)
branchName	gh_branch_name	Default	String

Issue Document

GitHub field name	Index field name	Description	Data type
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String

GitHub field name	Index field name	Description	Data type
issueNumber	gh_issue_number	Custom	Long (numeric)
issueTitle	gh_issue_title	Custom	String
owner	_authors	Default	String list
fileType	_file_type	Default	String
issueSourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
issueFileName	gh_file_name	Custom	String
issueState	gh_issue_state	Custom	String
issueLabel	gh_issue_labels	Default	String list
issueAssignee	gh_issue_assignee	Default	String list

Issue Comment

GitHub field name	Index field name	Description	Data type
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String
issueNumber	gh_issue_number	Custom	Long (numeric)
issueTitle	gh_issue_title	Custom	String
owner	_authors	Default	String list

GitHub field name	Index field name	Description	Data type
issueSourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
issueState	gh_issue_state	Custom	String
issueLabel	gh_issue_labels	Default	String list
issueAssignee	gh_issue_assignee	Default	String list

Issue Attachment

GitHub field name	Index field name	Description	Data type
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String
issueNumber	gh_issue_number	Custom	Long (numeric)
issueTitle	gh_issue_title	Custom	String
owner	_authors	Default	String list
issueSourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
issueFileName	gh_file_name	Custom	String
issueFileType	_file_type	Custom	String

GitHub field name	Index field name	Description	Data type
issueState	gh_issue_state	Custom	String
issueLabel	gh_issue_labels	Default	String list
issueAssignee	gh_issue_assignee	Default	String list

Pull Request Comment

GitHub field name	Index field name	Description	Data type
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String
PRNumber	gh_pr_number	Custom	Long (numeric)
PRTitle	gh_pr_title	Custom	String
owner	_authors	Default	String list
PRSourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
PRState	gh_pr_state	Custom	String
PRLabel	gh_pr_labels	Default	String list
PRAssignee	gh_pr_assignee	Default	String list

Pull Request Document

GitHub field name	Index field name	Description	Data type
repositoryName	gh_repository_name	Custom	String
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String
PRNumber	gh_number	Custom	Long (numeric)
PRTitle	gh_pr_title	Custom	String
owner	_authors	Default	String list
PRSourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
PRFileName	gh_file_name	Custom	String
PRFileType	_file_type	Custom	String
PRState	gh_pr_state	Custom	String
PRLabel	gh_pr_labels	Default	String list
PRAssignee	gh_pr_assignee	Default	String list

Pull Request Attachment

GitHub field name	Index field name	Description	Data type
repositoryName	gh_repository_name	Custom	String

GitHub field name	Index field name	Description	Data type
repositoryVisibility	gh_repository_visibility	Custom	String
category	_category	Default	String
PRNumber	gh_number	Custom	Long (numeric)
PRTitle	gh_pr_title	Custom	String
owner	_authors	Default	String list
PRSourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
PRFileName	gh_file_name	Custom	String
PRFileType	_file_type	Custom	String
PRState	gh_pr_state	Custom	String
PRLabel	gh_pr_labels	Default	String list
PRAssignee	gh_pr_assignee	Default	String list

IAM role for GitHub (Server) connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
```

```
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Gmail to Amazon Q Business

With Amazon Q Business, you can connect your Gmail enterprise email system to unlock valuable organizational knowledge stored in email communications. When you connect Gmail to Amazon Q Business, your users can search and get answers from email content and conversations directly through the Amazon Q web experience.

You can connect your Gmail instance to Amazon Q Business using either the AWS Management Console or the CreateDataSource API. This connection enables your organization to leverage email-based knowledge for improved decision-making and faster information discovery.

Topics

- Gmail connector versions
- Gmail connector overview
- Prerequisites for connecting Amazon Q Business to Gmail
- Connecting Amazon Q Business to Gmail using the latest connector (Console)
- Connecting Amazon Q Business to Gmail using the legacy connector (Console)

- Connecting Amazon Q Business to Gmail using the new connector (API)
- Connecting Amazon Q Business to Gmail using the original connector (API)
- How Amazon Q Business connector crawls Gmail ACLs
- Gmail data source connector field mappings
- IAM role for Amazon Q Business Gmail connector
- Understand error codes in the Amazon Q Business Gmail connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Gmail connector versions

Gmail offers two connector versions to meet different configuration needs:

Latest Gmail connector (Recommended)

> **Note**
>
> The latest connector provides improved accuracy. We recommend using the latest connector for new implementations. The legacy connector remains available for customers requiring specific features not yet supported in the latest connector.

The latest Gmail connector provides a simplified configuration experience with essential features:

- Configurable crawling of Email and Draft Email content
- Simplified filtering with only Date Range options
- Enhanced UI with improved validation and tips
- Automatic crawling of ACL and identity information

Legacy Gmail connector

The original Gmail connector provides full-featured configuration with advanced options:

- Complete entity type selection including Message attachments
- Advanced filtering options including domains, keywords, and labels
- Custom field mappings for metadata extraction
- Configurable sync modes and VPC settings
- Regex pattern matching for complex attachment filtering
- Manual ACL and identity crawling configuration

Gmail connector overview

The following table gives an overview of the Gmail connector and its supported features.

Category	Feature	Latest Connector	Legacy Connector
Security	**Authentication type**	Google Service Account	Google Service Account
	Authentication credentials	**Google service account** • Google service account • Admin account email • Client email • Private key	**Google service account** • Google service account • Admin account email • Client email • Private key
	Access Control List (ACL) crawling	Yes (Automatic)	Yes (Manual configuration)
	Identity crawling	Yes (Automatic)	Yes (Manual configuration)

Category	Feature	Latest Connector	Legacy Connector
	VPC	No	Yes
	Customer Managed Key (CMK) support	No	Yes
Crawl features	**Custom metadata**	No	No
	Entities	Messages (automatic), Draft emails (configurable)	Messages, Attachments (configurable)
	Field mappings	No (Uses optimized defaults)	Yes (Configurable)
	Filters	No	Date range, Attachments (regex), Domains, Keywords, Labels
Sync mode	Sync mode	No (Optimized automatic sync)	Yes (Full and incremental sync)

Prerequisites for connecting Amazon Q Business to Gmail

Before you connect Amazon Q Business to Gmail, you need to set up authentication and permissions in your Google Workspace environment. This setup ensures Amazon Q Business can securely access your email data while respecting your organization's access controls.

Setting up Google Workspace authentication

Complete these steps in your Google Workspace environment to prepare for the Amazon Q Business connection:

To set up Google Workspace authentication

1. Verify you have Google Workspace (not personal Gmail accounts).
2. Create a Google Cloud Platform admin account and Google Cloud project if you don't already have them.
3. Enable the Gmail API and Admin SDK API in your Google Cloud project:
    a. Go to the Google Cloud Console API Library.
    b. Search for and enable the Gmail API.
    c. Search for and enable the Admin SDK API.
4. Create a service account and download the JSON private key. For detailed instructions, see Create a service account key and Service account credentials in the Google Cloud documentation.
5. Configure OAuth scopes for your service account. Add these required scopes:
    - `https://www.googleapis.com/auth/admin.directory.user.readonly`
    - `https://www.googleapis.com/auth/admin.directory.group.readonly`
    - `https://www.googleapis.com/auth/gmail.readonly`
6. Save the following information for use in Amazon Q Business:
    - Admin account email address
    - Service account email address
    - Private key from the JSON file

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.

- Stored your Gmail authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Gmail using the latest connector (Console)

The following procedure outlines how to connect Amazon Q Business to Gmail using the latest connector and the AWS Management Console. The latest connector provides a simplified configuration experience with automatic ACL and identity crawling.

Connecting Amazon Q to Gmail using the latest connector

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Gmail** data source to your Amazon Q application.
5. Then, on the **Gmail** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. In **Authentication**, for **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your Gmail authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens.

   - Enter the following information in the **Create an AWS Secrets Manager secret window**:

     i. **Secret Name** – A name for your secret.

     ii. **Client email** – The client email address that you copied from your Google service account. For example, it might look like this:

     ```
     "{"clientEmailId":"service-
     account@123.iam.gserviceaccount.com","adminAccountEmailId":"admin@accounthost.com",
     "privateKey":"-----BEGIN PRIVATE KEY-----PRIVATE KEY HERE-----END PRIVATE
      KEY-----\n"}"
     ```

     iii. **Admin account email** – The admin account email address that you would like to use.

     iv. **Private key** – The private key that you copied from your Google service account.

     v. Choose **Save**.

8. For **Additional configuration – *optional***, configure the date range filter:

   - **Date range** – Configure the time period for crawling email messages. Choose from:

     - *Date range*: Specify start and end dates. **(optional)** - if not provided, the entire inbox is crawled.
     - *Start date onwards*: Specify only a start date to crawl from that date forward

   > **Note**
   >
   > **Simplified configuration:** The latest connector automatically crawls email content and allows configurable draft email crawling. Only date range filtering is available to keep the configuration simple and reliable.

9. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.

10. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.

11. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Gmail using the legacy connector (Console)

The following procedure outlines how to connect Amazon Q Business to Gmail using the legacy connector and the AWS Management Console. The legacy connector provides full-featured configuration with advanced options.

Connecting Amazon Q to Gmail using the legacy connector

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Gmail** data source to your Amazon Q application.
5. Then, on the **Gmail** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

> **Note**
>
> You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
8. In **Authentication**, for **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your Gmail authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens.

   - Enter the following information in the **Create an AWS Secrets Manager secret window**:

     i. **Secret Name** – A name for your secret.

     ii. **Client email** – The client email address that you copied from your Google service account.

     iii. **Admin account email** – The admin account email address that you would like to use.

     iv. **Private key** – The private key that you copied from your Google service account.

     v. Choose **Save**.
9. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

   > **Note**
   >
   > Creating a new service IAM role is recommended.

   For more information, see IAM role.
10. In **Sync scope**, choose from the following entity types:

- **Message attachments** – Choose to crawl email attachments. Messages are crawled by default.

11. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
12. For **Additional configuration – *optional***, configure the comprehensive filtering options available in the original connector:

    a. **Date range** – Enter a date range to specify the start and end date of email messages to be crawled.

    b. **Email domains** – Include or exclude email messages based on domains.

    c. **Keywords in subjects** – Include or exclude email messages based on keywords in their subjects.

    > **Note**
    >
    > You can also choose to include any documents that match all the subject keywords that you have entered.

    d. **Labels** – Add regular expression patterns to include or exclude specific labels. You can add up to 100 patterns.

    e. **Attachments** – Add regular expression patterns to include or exclude specific attachments. You can add up to 100 patterns.

13. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

    To extract audio transcriptions and video content, enable processing for the following file types:

14. For **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

15. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.

17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.

18. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

    For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Gmail using the new connector (API)

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

New Gmail connector JSON schema

The following is the new Gmail connector JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["GMAILV2"]
    },
    "connectionConfiguration": {
      "type": "object",
```

```
      "properties": {
        "secretArn": {
          "type": "string",
          "pattern": "^arn:[a-z0-9-\\.]{1,63}:[a-z0-9-\\.]{0,63}:[a-z0-9-\\.]{0,63}:[a-
z0-9-\\.]{0,63}:[^/].{0,1023}$"
        }
      },
      "required": ["secretArn"]
    },
    "dataEntityConfiguration": {
      "type": "object",
      "properties": {
        "crawlDraftEmails": {
          "type": "boolean"
        }
      }
    },
    "filterConfiguration": {
      "type": "object",
      "properties": {
        "maxFileSizeInMegaBytes": {
          "type": "string",
          "pattern": "^\\d+$"
        },
        "startDateFilter": {
          "type": "string",
          "format": "date-time"
        },
        "endDateFilter": {
          "type": "string",
          "format": "date-time"
        }
      }
    },
    "deletionProtectionConfiguration": {
      "type": "object",
      "properties": {
        "enableDeletionProtection": {
          "type": "boolean"
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "pattern": "^(100|[1-9][0-9]?)$"
        }
```

```
      },
      "required": ["enableDeletionProtection", "deletionProtectionThreshold"]
    }
  },
  "required": [
    "type",
    "connectionConfiguration",
    "dataEntityConfiguration"
  ]
}
```

The following table provides information about important JSON keys to configure for the new Gmail connector.

Configuration	Description
`type`	The type of data source. Specify `GMAILV2` for the new Gmail connector.
`connectionConfiguration`	Configuration information for connecting to the Gmail data source.
`secretArn`	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains the key-value pairs required to connect to your Gmail. The secret must contain a JSON structure with the following keys: `{ "adminAccountEmailId": "${adminAccountEmailId}" , "clientEmailId": "${clientEmailId}" , "privateKey": "${privateKey}" }`
`dataEntityConfiguration`	Configuration for the types of data entities to crawl.

Configuration	Description
`crawlDraftEmails`	A Boolean value to choose whether you want to crawl draft messages. Default is `false`.
`filterConfiguration`	Optional filtering configuration for the data source.
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
`startDateFilter`	Specify messages to be included from a certain start date onwards. Use ISO 8601 date-time format.
`endDateFilter`	Specify messages to be included up to a certain end date. Use ISO 8601 date-time format.
`deletionProtectionConfiguration`	Configuration for deletion protection to prevent accidental data loss.
`enableDeletionProtection`	A Boolean value to enable deletion protectio n. When enabled, prevents deletion of more than the specified threshold percentage of documents.
`deletionProtectionThreshold`	The maximum percentage (1-100) of documents that can be deleted in a single sync. Required when deletion protection is enabled.

Connecting Amazon Q Business to Gmail using the original connector (API)

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Original Gmail connector JSON schema

The following is the original Gmail connector JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
      }
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "message": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
```

```
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        }
      },
      "attachments": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
```

```
          }
        }
      },
      "required": []
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "isCrawlAcl": {
          "type": "boolean"
        },
        "fieldForUserId": {
          "type": "string"
        },
        "inclusionLabelNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionLabelNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionAttachmentTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionAttachmentTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionAttachmentNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
```

```
        "exclusionAttachmentNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionSubjectFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionSubjectFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "isSubjectAnd": {
          "type": "boolean"
        },
        "inclusionFromFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFromFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionToFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionToFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
```

```
        },
        "inclusionCcFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionCcFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionBccFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionBccFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "beforeDateFilter": {
          "anyOf": [
            {
              "type": "string",
              "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
            },
            {
              "type": "string",
              "pattern": ""
            }
          ]
        },
        "afterDateFilter": {
          "anyOf": [
            {
              "type": "string",
              "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
            },
            {
```

```
            "type": "string",
            "pattern": ""
          }
        ]
      },
      "isCrawlAttachment": {
        "type": "boolean"
      },
      "shouldCrawlDraftMessages": {
        "type": "boolean"
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
      }
    },
    "required": [
      "isCrawlAttachment",
      "shouldCrawlDraftMessages"
    ]
  },
  "type" : {
    "type" : "string",
    "pattern": "GMAIL"
  },
  "syncMode": {
    "type": "string",
    "enum": [
      "FORCED_FULL_CRAWL",
      "FULL_CRAWL"
    ]
  },
  "enableIdentityCrawler": {
    "type": "boolean"
  },
  "secretArn": {
    "type": "string",
    "minLength": 20,
    "maxLength": 2048
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
```

```
        }
      ]
    }
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties",
    "syncMode",
    "secretArn",
    "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the endpoint for the data source.
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings. Specify the type of data source and the secret ARN.
• `message` • `attachments`	A list of objects that map the attributes or field names of your Gmail messages and attachments to Amazon Q index field names.
`additionalProperties`	Additional configuration options for your content in your data source.
`isCrawlAcl`	Specify `true` to crawl access control informati on from documents.

Configuration	Description
	Note Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.
• `inclusionLabelNamePatterns` • `exclusionLabelNamePatterns` • `inclusionAttachmentTypePatterns` • `exclusionAttachmentTypePatterns` • `inclusionAttachmentNamePatterns` • `exclusionAttachmentNamePatterns` • `inclusionSubjectFilter` • `exclusionSubjectFilter` • `inclusionFromFilter` • `exclusionFromFilter` • `inclusionToFilter` • `exclusionToFilter` • `inclusionCcFilter` • `exclusionCcFilter` • `inclusionBccFilter` • `exclusionBccFilter`	A list of regular expression patterns to include or exclude messages with specific subject names in your Gmail data source. Files that match the patterns are included in the index. If a file matches both an inclusion and an exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.

Configuration	Description
isSubjectAnd	true to index.
beforeDateFilter	Specify messages and attachments to be included before a certain date.
afterDateFilter	Specify messages and attachments to be included after a certain date.
isCrawlAttachment	A Boolean value to choose whether you want to crawl attachments. Messages are automatic ally crawled.
maxFileSizeInMegaBytes	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
type	The type of data source. Specify GMAIL as your data source type.
shouldCrawlDraftMessages	A Boolean value to choose whether you want to crawl draft messages.

Configuration	Description
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose from the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index **Important** Because there is no API to update permanently deleted Gmail messages, a **New, modified, or deleted content sync** does *not* do the following: • Remove messages that were permanently deleted from Gmail from your Amazon Q index • Sync changes in Gmail email labels To sync your Gmail data source label changes and permanently deleted email messages to your Amazon Q index, you must run full crawls periodically.

Configuration	Description
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/principal informati on on users and groups with access to specific documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.
`secretARN`	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains the key-value pairs required to connect to your Gmail. The secret must contain a JSON structure with the following keys: `{ "adminAccountEmailId": "${adminAccountEmailId}" , "clientEmailId": "${clientEmailId}" , "privateKey": "${privateKey}" }`
`version`	The version of the template that's currently supported.

How Amazon Q Business connector crawls Gmail ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an Gmail data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your Gmail instance. ACL crawling behavior differs between the two Gmail connector versions.

> **Note**
>
> **ACL behavior by connector version:**
>
> - **Latest connector:** ACL and identity crawling is automatically enabled and cannot be disabled. Only applies to email messages and draft emails - attachments are not supported.
> - **Legacy connector:** ACL and identity crawling can be manually configured during setup. Applies to both messages and attachments when attachment crawling is enabled.

The legacy Gmail connector for Amazon Q Business crawls 2 primary content types: messages (email along with metadata such as subject, from, or to) and attachments. Each email message (in sent and inbox) and its respective attachments is considered as a separate document with distinct document IDs. Currently, the connector cannot associate an attachment with its parent message, even though attachments inherit permissions from parent messages.

> **Note**
>
> **Latest connector limitations:** The latest Gmail connector does not support attachment crawling. The latest Gmail connector does not support attachment crawling. If your organization requires attachment indexing, use the legacy connector instead.

Permission Inheritance: ACLs for messages are set based on user email addresses. **Legacy connector only:** Attachments automatically inherit permissions from parent email messages when attachment crawling is enabled.

ACL indexing: Individual user synchronization is supported based on email addresses, and domain-wide access is supported using service account authentication.

Change Management: ACL changes are supported in both Full Crawl and Incremental or Change Log modes.

Failure handling The connector implements a fail-close approach for API failures, with rate limiting handled through queue-based wait time with exponential backoff. When permissions issues occur, documents are skipped from ingestion rather than being made publicly accessible.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

> **Note**
>
> **ACL behavior by connector version:**
>
> - **New connector:** ACL and identity crawling is automatically enabled and cannot be disabled. No manual configuration is required.
> - **Original connector:** ACL and identity crawling can be manually configured during setup.

Gmail data source connector field mappings

You can improve search results and customize your users' chat experience by mapping document attributes from your Gmail data to fields in your Amazon Q index.

With Amazon Q, you can map two types of attributes to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have an attribute mapping already available, or if you want to map additional document attributes to index fields, you can use custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after you create your application and retriever.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

Important

Filtering using document attributes in chat is only supported through the API.

The Amazon Q Gmail connector supports the following entities and the associated reserved and custom attributes.

Supported entities and field mappings

- Messages

Messages

Gmail field name	Index field name	Description	Data type
category	_category	Default	String
internalDate	_created_at	Default	Date
id	gmail_message_is	Custom	String
labelIds	gmail_message_label_ids	Custom	String list
historyId	gmail_message_history_id	Custom	String
subject	gmail_subject	Custom	String

Gmail field name	Index field name	Description	Data type
from	gmail_from	Custom	String
to	gmail_to	Custom	String list
cc	gmail_cc	Custom	String list
bcc	gmail_bcc	Custom	String list

Note

Original connector only: Field mappings are only available when using the original Gmail connector. The new connector uses optimized default field mappings that cannot be customized.

IAM role for Amazon Q Business Gmail connector

Note

Applies to both connector versions: The IAM role requirements are the same for both the new and original Gmail connectors. However, the new connector automatically handles VPC configurations, while the original connector allows manual VPC setup.

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
```

```
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
```

```
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
```

```
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see [IAM roles for Amazon Q data source connectors](#).

Understand error codes in the Amazon Q Business Gmail connector

The following table provides information about error codes you may see for the Gmail connector and suggested resolutions.

Error code	Error message	Suggested resolution
GML-5001	There was a problem while retrieving directory .	There was a problem while retrieving directory because of incorrect credentia ls. Provide correct credentials and try again.
GML-5002	There was a problem while retrieving user specific Gmail object.	There was a problem while retrieving user specific Gmail object because of incorrect credentials. Provide correct credentials and try again.
GML-5003	Connection lost - A problem occurred while validating credentials.	Connection was lost due to invalid credentials. Provide correct credentials and try again.
GML-5004	There was a problem while retrieving the user list because the API was not responding.	There was a problem while retrieving the user list because the API was not responding. Try again.
GML-5100	There was a problem while retrieving repositor y configurations. Repository configura tions may be empty or incorrect.	Repository configurations should not be empty or incorrect. Provide valid details for repository configurations.
GML-5101	There was a problem while retrieving message entity from repositor y configurations. No message entity found	Message entity should not be empty. Check if message entity is present in repository configurations and provide the same if not present.

Error code	Error message	Suggested resolution
	in repository configura tions.	
GML-5102	There was a problem while retrieving attachment entity from repository configura tions. No attachment entity found in repositor y configurations.	Attachment entity should not be empty. Check if attachment entity is present in repository configurations and provide the same if not present.
GML-5103	There was a problem while retrieving field mappings for message entity from repositor y configurations. Field mappings may be empty or incorrect.	Field mappings should not be empty or incorrect. Provide proper field mappings for message entity in repository configurations.
GML-5104	There was a problem while retrieving field mappings for attachmen t entity from repositor y configurations. Field mappings may be empty or incorrect.	Field mappings should not be empty or incorrect. Provide proper field mappings for message entity in repository configurations.
GML-5105	There was a problem while retrieving field mapping values for message entity. Field mapping values may be empty or incorrect.	Field mappings values should not be empty or incorrect. Provide proper field mapping values for message entity in repository configurations.

Error code	Error message	Suggested resolution
GML-5106	There was a problem while retrieving field mapping values for attachment entity. Field mapping values may be empty or incorrect.	Field mappings values should not be empty or incorrect. Provide proper field mapping values for message entity in repository configurations.
GML-5107	There was a problem while parsing before/after date filter value. Before/After date format may be incorrect.	Provide correct before/after date format. E.g. yyyy-MM-ddTHH:mm:ssZ.
GML-5108	There was a problem while retrieving client email id. Client email id may be empty or incorrect.	The client email id should not be empty or incorrect. Provide correct client email id.
GML-5109	There was a problem while retrieving admin account email id. Admin account email id may be empty or incorrect.	The admin account email id should not be empty or incorrect. Provide correct admin account email id.
GML-5110	There was a problem while retrieving private key. Private key may be empty or incorrect.	The private key should not be empty or incorrect. Provide correct private key.
GML-5111	One or more of the provided filter regex are invalid.	Provide correct regex value in filter fields.

Error code	Error message	Suggested resolution
GML-5200	There was a problem while retrieving Gmail items.	There was a problem while retrievin g Gmail items because user is not provided. Ensure that user is not empty.
GML-5201	There was a problem while retrieving the message body because the API was not responding.	There was a problem while retrieving the message body because the API was not responding. Try again.
GML-5202	There was a problem while retrieving the message subject because the API was not responding.	There was a problem while retrieving the message subject because the API was not responding. Try again.
GML-5203	There was a problem while retrieving the attachment because the API was not responding.	There was a problem while retrieving the attachment because the API was not responding. Try again.
GML-5204	There was a problem while retrieving the message metadata because the API was not responding.	There was a problem while retrieving the message metadata because the API was not responding. Try again.
GML-5205	There was a problem while retrieving the attachment metadata because the API was not responding.	There was a problem while retrieving the attachment metadata because the API was not responding. Try again.

Error code	Error message	Suggested resolution
GML-5206	There was a problem while retrieving the message because the API was not responding.	There was a problem while retrieving the message because the API was not responding. Try again.
GML-5500	Connection timed out - API is not responding. The threshold number of API calls has been exceeded.	Timeout exception occurred due to API not responding. The threshold number of API hits has been exceeded. Try again.

Connecting Google Calendar to Amazon Q Business (Preview)

> **Note**
>
> The Google Calendar connector is in preview release and is subject to change.

Google Calendar is an online calendar tool developed by Google. You can connect a Google Calendar instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the Google Calendar connector (Preview)
- Google Calendar connector overview (Preview)
- Prerequisites for connecting Amazon Q Business to Google Calendar (Preview)
- Connecting Amazon Q Business to Google Calendar using the console (Preview)
- Connecting Amazon Q Business to Google Calendar using APIs
- How Amazon Q Business connector crawls Google Calendar ACLs
- Google Calendar data source connector field mappings
- IAM role for Amazon Q Business Google Calendar connector (Preview)
- Understand error codes in the Amazon Q Business Google Calendar connector (Preview)

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Google Calendar connector (Preview)

The connector employs a rolling window approach for indexing data. This rolling window mechanism spans a total of six months, with four months of historical data and two months of future data. As the connector syncs and ingests new data, the oldest data that falls beyond the four-month historical window is automatically purged from the index. Simultaneously, new data for the upcoming two months is added to the index, allowing for future data visibility and analysis.

Google Calendar connector overview (Preview)

The following table gives an overview of the Google Calendar connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Google Service Account and OAuth 2.0
	Authentication credentials	**Google service account** • Google service account • Admin account email • Client email • Private key OAuth 2.0 • Client ID • Client secret

Category	Feature	Support
		• Refresh token
	Access Control List (ACL) crawling	Yes
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	No
	Entities	Yes. The following entities are supported: • Calendar • Events See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports default field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include/Exclude calendars by email address
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Google Calendar (Preview)

Before you begin, make sure that you have completed the following prerequisites.

In Google Calendar, make sure you have:

- Created a Google Cloud Platform admin account and have created a Google Cloud project.
- Activated the Google Calendar API and Admin SDK API in your admin account.

- Created a service account and downloaded a JSON private key for your Google Calendar. For information about how to create and access your private key, see Create a service account key and Service account credentials on the Google Cloud website.

On the Google Cloud website:

- Copied your admin account email, your service account email, and your private key to use for authentication.
- Added the following Oauth scopes, using an admin role, for your user and the shared directories you want to index:
  - https://www.googleapis.com/auth/admin.directory.user.readonly
  - https://www.googleapis.com/auth/gmail.readonly

  In your AWS account, make sure you have:
  - Created an Amazon Q Business application.
  - Created an Amazon Q Business retriever and added an index.
  - Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
  - Stored your Google Calendar authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Google Calendar authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Google Calendar using the console (Preview)

The following procedure outlines how to connect Amazon Q Business to Google Calendar using the AWS Management Console.

Connecting Amazon Q to Google Calendar

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Google Calendar** data source to your Amazon Q application.
5. Then, on the **Google Calendar** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
8. In **Authentication**, Choose between Google service account or OAuth 2.0 authentication, based on your use case.
9. AWS Secrets Manager secret – Choose an existing secret or create a Secrets Manager secret to store your Google Calendar authentication credentials. If you choose to create a secret, an **AWS Secrets Manager secret** window opens.

a. If you choose **Existing**, select an existing secret for **Select secret**.

b. If you choose New, enter the following information in the New AWS Secrets Manager secret section:

   i. **Secret Name** – A name for your secret.

   ii. If you chose Google service account, enter the following information:

      A. **Client email** – The email ID of the service account.

      B. **Admin account email** –The email ID of the admin user (the email used by the Service Account User) in your Google service account configuration.

      C. **Private key** – The private key created in your Google service account.

      D. Choose **Save and add secret**.

c. If you chose OAuth 2.0 authentication, enter the details of Secret Name, Client ID, Client secret and Refresh token that you created in your service account. Then, choose Save and add secret.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

    For more information, see IAM role.

12. In Sync scope, choose from the following options:

- **All calendars**: Add all the calendars to the index.
- **Specific calendars only**: Add email addresses associated to only the calendars you want to include in your index.
- **Exclude specific calendars**: Add email addresses for the calendars you want to exclude from your index.

13. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. For **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

15. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
16. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
17. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

18. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Google Calendar using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- Google Calendar configuration properties
- Google Calendar JSON schema

- Google Calendar JSON schema example

Google Calendar configuration properties

The following table provides information about configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the data source.	`object` This property has the following sub-property: `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source. This data source doesn't specify an endpoint. You choose your authentication type: `serviceAccount` and `OAuth2`. The connection information is included in an AWS Secrets Manager secret that you provide the `secretArn` .	`object` This property has the following sub-property: `authType`.	Yes
`authType`	Choose between `serviceAccount` and `OAuth2`, based on your use case.	`string`	Yes

Configuration	Description	Type	Required
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties: `file` and `comment`.	Yes
• 1) Calendar • 2) Event	A list of objects that map the attributes or field names of your Google calendar to Amazon Q index field names.	`object` `object` These properties have the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName` • `dateFieldFormat`	No
`indexFieldName`	The field name of your Google Drive to Amazon Q index field names.	`string`	Yes
`indexFieldType`	The field type of your Google Drive to Amazon Q index field names.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes

Configuration	Description	Type	Required
`dataSourceFieldName`	The data source field name of your Google Calendar to Amazon Q index field names.	`string`	Yes
`dateFieldFormat`	The date format of your Google Calendar to Amazon Q index field names.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No
`additionalProperties`	Additional configuration options for your content in your data source	`object` This property has the following sub-properties. • `isCrawlAcl` • `fielForUserId` • `InclusionUserList` • `exclusionUserList` • `enableDeletionProtection` • `DeletionProtectionThreshold`	Yes

Configuration	Description	Type	Required
`isCrawlAcl`	Specify `true` to crawl access control informati on by default from documents. **Note** Amazon Q Business crawls ACL information to ensure responses are generated only from documents your end users have access to. See Authoriza tion for more details.	`boolean`	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No

Configuration	Description	Type	Required
`inclusionUsersList` `exclusionUsersLists`	A list of email IDs to exclude specific users from your Google Calendardata source. Users whose email IDs match these will be excluded from the index, while users whose email IDs do not match will be included. If a file matches both an exclusion and an inclusion, the exclusion takes precedence, and the file will not be included in the index.	`array`	No
• `type`	The type of source. We recommend GOOGLECALENDAR as your data source type.	`string` Valid values are GOOGLECALENDAR.	No

Configuration	Description	Type	Required
• `enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to certain documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls ACL information to ensure responses are generated only from documents your end users have access to. See Authorization for more details.	`boolean`	Yes

Configuration	Description	Type	Required
• `syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	`string` You can choose between the following options: Use `FORCED FULL CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your indexUse.Use `FULL CRAWL` to increment ally crawl only new, modified, and deleted content each time your data source syncs with your index	Yes

Configuration	Description	Type	Required
• SecretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Google Drive. .	string The secret must contain a JSON structure with the following keys: If using Google Service Account authentication: {"clientEmail": "user account email","adminAccountEmail": "service account email","privateKey": "private key"}If using OAuth 2.0 authentication: {"clientID": "OAuth client ID","clientSecret" : "client secret","refreshToken": "refresh token"}	No
• version	The version of this template that's currently supported.	string	No

Google Calendar JSON schema

The following is the Google Calendar JSON schema:

```
{

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "authType": {
              "type": "string",
              "enum": [
                "OAuth2",
                "serviceAccount"
              ]
            }
          },
          "required": [
            "authType"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "calendar": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
```

```
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "DATE",
                      "STRING_LIST",
                      "LONG"
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        }
      },
      "event": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
```

```
                    "type": "string",
                    "enum": [
                      "STRING",
                      "DATE",
                      "STRING_LIST"
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        }
      }
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "fieldForUserId": {
          "type": "string"
        },
        "isCrawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": [
                "true",
                "false"
              ]
```

```
            }
          ]
        },
        "inclusionUsersList": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionUsersList": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "type": "boolean",
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      }
    },
    "enableIdentityCrawler": {
      "type": "boolean"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FULL_CRAWL",
        "FORCED_FULL_CRAWL"
      ]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "type": {
      "type": "string",
      "pattern": "GOOGLECALENDAR"
    },
```

```
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
  ]
}
```

Google Calendar JSON schema example

The following is the Google Calendar JSON schema example:

```
{

{
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "authType": "serviceAccount"
    }
  },
  "repositoryConfigurations": {
    "calendar": {
      "fieldMappings": [
        {
          "indexFieldName": "_category",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "category"
        },
        {
          "indexFieldName": "_source_uri",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "sourceUrl"
```

```
        }
      ]
    },
    "event": {
      "fieldMappings": [
        {
          "indexFieldName": "_category",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "category"
        },
        {
          "indexFieldName": "gcal_location",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "location"
        },
        {
          "indexFieldName": "_created_at",
          "indexFieldType": "DATE",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'",
          "dataSourceFieldName": "created"
        },
        {
          "indexFieldName": "_last_updated_at",
          "indexFieldType": "DATE",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'",
          "dataSourceFieldName": "updated"
        },
        {
          "indexFieldName": "gcal_event_start_time",
          "indexFieldType": "DATE",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'",
          "dataSourceFieldName": "eventStartTime"
        },
        {
          "indexFieldName": "gcal_event_end_time",
          "indexFieldType": "DATE",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'",
          "dataSourceFieldName": "eventEndTime"
        },
        {
          "indexFieldName": "_source_uri",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "htmlLink"
        },
```

```
        {
          "indexFieldName": "gcal_organizer",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "organizer"
        },
        {
          "indexFieldName": "gcal_attendees",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "attendees"
        },
        {
          "indexFieldName": "gcal_recurrence",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "recurrence"
        }
      ]
    }
  },
  "additionalProperties": {
    "fieldForUserId": "email",
    "isCrawlAcl": true,
    "inclusionUsersList": [
      "ABC"
    ],
    "exclusionUsersList": [
      "TEST"
    ],
    "enableDeletionProtection": true,
    "deletionProtectionThreshold": "2"
  },
  "type": "GOOGLECALENDAR",
  "syncMode": "FORCED_FULL_CRAWL",
  "enableIdentityCrawler": true,
  "secretArn": "arn:aws::secretsmanager:us-west-2:123:secret:AmazonKendra-
GoogleCalendar",
  "version": "1.0.0"
}
```

How Amazon Q Business connector crawls Google Calendar ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an Google Calendar data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your Google Calendar instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Google Calendar data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Google Calendar connector supports the following entities and field mappings.

Supported entities and field mappings

- Files

Files

Calendar

Google Calendar field name	Index field name	Description	Data type
sourceUrl	_sourceUrl	Default	String

Events

Google Calendar field name	Index field name	Description	Data type
Location	gcal_location	Custom	String
eventStartTime	gcal_event_start_time	Custom	Date
eventEndTime	gcal_event_end_time	Custom	Date
category	_category	Default	String
created	_created_at	Default	DateString

Google Calendar field name	Index field name	Description	Data type
updated	_last_updated_at	Default	Date
htmlLink	_source_url	Default	String
attendees	gcal_attendees	Custom	String
organizer	gcal_organizer	Custom	String
recurrence	gcal_recurrence	Custom	String

IAM role for Amazon Q Business Google Calendar connector (Preview)

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
```

```
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
```

```
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
```

```
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the Amazon Q Business Google Calendar connector (Preview)

The following table provides information about error codes you may see for the Google Calendar connector and suggested resolutions.

Error code	Error message	Suggested resolution
GCAL-5001	Connection lost - A problem occurred while validating credentials	A problem occurred while validating credentials. Provided credentials may be incorrect.

Error code	Error message	Suggested resolution
GCAL-5002	There was a problem while retrieving the directory	There was a problem while retrieving the directory due to incorrect credentia ls. Provide correct credentials and try again.
GCAL-5003	Connection lost - A problem occurred while validating credentials.	Connection was lost due to invalid credentials. Provide correct credentials and try again.
GCAL-5004	There was a problem while retrieving the user list because the API was not responding.	There was a problem while retrieving the user list because the API was not responding. Try again.
GCAL-5100	There was a problem while generating the new access token.	
GCAL-5101	There was a problem while retrieving the private key.	The private key may be empty or incorrect.
GCAL-5102	There was a problem while retrieving the http request initializer.	
GCAL-5103	Auth Type can not be null or empty	Enter a valid value.
GCAL-5104	Invalid value for Auth Type	Enter a valid value.
GCAL-5105	Only String, String List, Date and Long formats are supported for the indexFieldType in all the field mappings.	Please provide the supported format only for the indexFieldType in all the fieldMappings.

Error code	Error message	Suggested resolution
GCAL-5106	There was a problem while retrieving client email id. Client email id may be empty or incorrect.	Client email id can not be empty or incorrect. Provide the proper values.
GCAL-5107	Client Email ID length is more than the size limit.	Client Email should be less than 255 characters.
GCAL-5108	There was a problem while retrieving admin account email id. Admin account email id may be empty or incorrect.	The admin account email id should not be empty or incorrect. Provide the correct email id.
GCAL-5109	Admin Account Email ID length is more than the size limit.	Admin Email should be less than 255 characters.
GCAL-5110	There was a problem while retrieving client id. Client id is empty or incorrect	The client id should not be empty or incorrect. Provide the correct email id.
GCAL-5111	There was a problem while retrieving client secret. Client secret is empty or incorrect	Enter a valid value.
GCAL-5112	There was a problem while retrieving refresh token. Refresh token is empty or incorrect	Provide the correct refresh token.

Error code	Error message	Suggested resolution
GCAL-5113	The connection configuration in your data source configuration is missing.	Enter valid connection configuration details and try again.
GCAL-5114	The repository endpoint metadata in your data source configuration is missing.	Enter valid repository endpoint metadata details and try again.
GCAL-5115	The repository credentials in your data source configuration is missing.	Enter valid repository credentials details and try again.
GCAL-5116	Invalid client email	Enter valid client email and try again.
GCAL-5117	Invalid admin account email	Enter valid admin account email and try again.
GCAL-5118	There was an error parsing the field value for field %s.	Size has exceeded the maximum allowable limit. The maximum size permitted is 1000.
GCAL-5119	There was an error parsing the field value. The size of the filter pattern exceeded the maximum number of characters allowed.	The maximum size permitted is 1000.
GCAL-5400	The identity crawler connection configuration in your data source configuration is missing.	Enter valid identity crawler connection configuration details and try again.

Error code	Error message	Suggested resolution
GCAL-5401	The identity crawler repository endpoint metadata in your data source configuration is missing.	Enter valid identity crawler repository endpoint metadata details and try again.
GCAL-5402	The identity crawler repository credentials in your data source configuration is missing.	Enter valid identity crawler repository credentials details and try again.
GCAL-5403	Auth Type can not be null or empty	Enter a valid value.
GCAL-5404	Invalid value for Auth Type	Enter a valid value.
GCAL-5500	Connection timed out - API is not responding.	The threshold number of API hits has been exceeded.

Connecting Google Drive to Amazon Q Business

Google Drive is a cloud-based file storage service. Amazon Q Business can connect to your Google Drive instances. You can connect Google Drive instance to Amazon Q—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

After you integrate Amazon Q with Google Drive, users can ask questions about content stored in their Google Drive. For example, users can inquire about key findings from Google Docs, presentation highlights from Google Slides, or search for specific information across multiple document types. The integration enables users to quickly access and understand information from their Google Drive content, regardless of file location or type, while providing contextual details such as publication dates, modification history, and document ownership—all contributing to more efficient information discovery and better-informed decision making.

Topics

- Connecting Google Drive to Amazon Q Business (New)

- Connecting Google Drive to Amazon Q Business (Original)

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Connecting Google Drive to Amazon Q Business (New)

With the new connector, you can build and refresh your index significantly faster than before, control the sync scope using a date filter, and enable your end-users to get insights from link sharing-enabled documents that they have accessed before. The new Google Drive connector also performs targeted identity crawls, eliminating the need to crawl all groups within an enterprise.

Known limitations for the Amazon Q Business Google Drive connector

The Amazon Q Google Drive connector new has the following known limitations:

- Comments synchronization is not supported in the new version.
- VPC connectivity is not supported.
- Custom field mappings are not supported.
- File type pattern filtering is not supported (use MIME type filtering instead).
- Document enrichment is not supported.

Google Drive connector overview

The following table gives an overview of the Amazon Q Business Google Drive connector new and its supported features.

Category	Feature	Support
Security	**Authentication type**	Service Account Based
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes.
Crawl features	**Entities**	Yes. The following entities are supported: • Files See What is a document? for more details on what each connector crawls as a document.
	Filters	Yes. The following filters are supported: • Include/exclude by shared drive IDs • Include/exclude by MIME types (e.g., `application/pdf` , `application/vnd.google-apps.document`) • Date range filtering
	File types	Supports all file types supported by Amazon Q. For more information see Doc types.

Prerequisites for connecting Amazon Q Business to Google Drive

Before you begin, make sure that you have completed the following prerequisites.

In Google Drive, make sure you have:

- **Either** been granted access by a super admin role **or** are a user with administrative privileges. You do not need a super admin role for yourself if you have been granted access by a super admin role.

- Configured Google Drive Service Account connection credentials containing your admin account email, client email (service account email), and private key. See Google Cloud documentation on creating and deleting service account keys.
- Created a Google Cloud Service Account (an account with delegated authority to assume a user identity) with **Enable G Suite Domain-wide Delegation** activated for server-to-server authentication, and then generated a JSON private key using the account.

> **Note**
>
> The private key should be generated after the creation of the service account.

- Added Admin SDK API and Google Drive API in your user account.
- Added (or asked a user with a super admin role to add) the following OAuth scopes to your service account using a super admin role. These API scopes are needed to crawl all documents, and access control (ACL) information for all users in a Google Workspace domain:
  - https://www.googleapis.com/auth/drive.readonly—View and download all your Google Drive files
  - https://www.googleapis.com/auth/drive.metadata.readonly—View metadata for files in your Google Drive
  - https://www.googleapis.com/auth/admin.directory.group.readonly—Scope for only retrieving group, group alias, and member information. This is needed for the Amazon Q Identity Crawler.
  - https://www.googleapis.com/auth/admin.directory.user.readonly—Scope for only retrieving users or user aliases. This is needed for listing users in the Amazon Q Identity Crawler and for setting ACLs.
  - https://www.googleapis.com/auth/cloud-platform—Scope for generating access token for fetching content of large Google Drive files.
  - https://www.googleapis.com/auth/forms.body.readonly—Scope for fetching data from Google Forms.

  To support the Forms API, add the following additional scope:

  - https://www.googleapis.com/auth/forms.body.readonly

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Google Drive authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Google Drive using the console

The following procedure outlines how to connect Amazon Q Business to Google Drive new using the AWS Management Console.

Connecting Amazon Q to Google Drive new

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Google Drive** data source to your Amazon Q application.
5. Then, on the **Google Drive** data source page, enter the following information:
6. **Name and description**, do the following:

    - For **Data source name** – Name your data source for easy tracking.

    > **Note**
    >
    > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. In **Authorization**, configure access control settings: Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting *Enable ACLs* to enable ACLs or *Disable ACLs* to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorizationfor more details.
8. **AWS Secrets Manager secret** – Choose an existing secret or create a secret to store your GoogleDrive authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens.

   - If you choose **Existing**, select an existing secret for **Select secret**.

     If you choose **New**, enter the following information in the **New AWS Secrets Manager secret** section:

     i. **Secret name** – A name for your secret.

     ii. Enter the following information:

     - **Secret Name** – A name for your secret.
     - **Admin account email** – The email ID of the admin user (the email used by the Service Account User) in your Google service account configuration.
     - **Client email** – The email ID of the service account.
     - **Private Key** – The private key created in your service account.

     Then, choose **Save and add secret**.
9. In **Identity crawler**, configure identity crawling settings:

   a. **Identity crawling has been turned on for your connector as the ACLs are enabled** – This notification appears when ACLs are enabled.

   b. **Manage identity crawling logs** – When enabled, CloudWatch logs will show identities associated with local groups, as crawled during each sync job. If you disable this option post sync job completion (or partial run), you'll need to manually delete any associated identity crawling logs already generated.

- **Enable identity crawling logs** – Identities crawled during data source sync will be logged.
- **Disable identity crawling logs** – Identities crawled during data source sync will not be logged.

10. **IAM role** – Amazon Q Business requires an IAM role to access repository credentials and application content:

    - **Choose an option** – Select an existing IAM role or create a new one.

11. In **Sync scope**, configure which content to sync:

    a. **Sync contents** – Choose the following options to select contents to sync. To further limit the contents that you want to sync for specific folders or files use the 'Entity regex patterns':

    - **My Drive** – Selected by default. Use this option if you want the files in all of your users' My Drives to be included.
    - **Shared with me** – Selected by default. Use this option if you want the files from 'Shared with me' to be included.
    - **Shared Drives** – Selected by default. Use this option if you want to include shared drives. You can use the shared drive filter (see below) to sync files from specific shared drives.

    b. For **Maximum file size** – You can specify the file size limit in GB for Amazon Q crawling. Amazon Q crawls only files within the defined size limit. The default file size is 50MB. The maximum file size limit is 10 GB. Files must be larger than 0 MB and no larger than 10 GB. You can go up to 10 GB (10240 MB) if you enable **Video files** in **Multi-media content** configuration, and up to 2 GB (2048 MB) if you enable **Audio files** in **Multi-media content configuration**.

12. In **Additional configuration - *optional***, configure additional filtering options. All content will be indexed by default. However, you can also limit the scope with these additional options:

    a. **Date filter** – Add a date range to filter content based on the last modified date:

    - **Start date** – Enter the start date in YYYY/MM/DD format.
    - **End date - *optional*** – Enter the end date in YYYY/MM/DD format.

    b. **Shared drives** – Add IDs of shared drives you want to include or exclude in your application:

- **Include shared drives** – Add shared drive IDs to include.
- **Exclude shared drives** – Add shared drive IDs to exclude.

c. **Mime types** – Add Mime types to include or exclude in Google Drive account:

- **Include mime types** – Add MIME types to include (e.g., `application/vnd.google-apps.document` for Google Docs, `application/pdf` for PDF files).
- **Exclude mime types** – Add MIME types to exclude.

d. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**. For more information, see Extracting semantic meaning from embedded images and visuals.

To extract audio transcriptions and video content, enable **Audio Files**. To extract video content, enable **Video files**. For more information, see Extracting semantic meaning from audio and video Content.

e. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

13. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
14. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
15. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.

You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
For more information, see Troubleshooting data source connectors.

IAM role for Amazon Q Business Google Drive connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
```

```
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:{{secret_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/{{key_id}}"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
    },
    {
      "Sid": "AllowsAmazonQToCallPrincipalMappingAPIs",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
```

```
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

How Amazon Q Business connector crawls Google Drive ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

The Google Drive connector for Amazon Q Business crawls files with enhanced performance. It supports various file formats, including spreadsheets, presentations, images, audio/video files, and Google Docs™.

Roles/permissions: The Google Drive connector translates Google Drive permissions into ACLs that are compatible with Amazon Q Business. There are four primary roles with permissions:

- Owner - Has full control.
- Editor - Can modify content, update metadata, and add or remove comments.
- Commenter - Can view content and add comments.
- Viewer - Has read-only access.

Permission Inheritance: The Google Drive connector is designed to detect and handle hierarchical content organization across My Drive and Shared Drives with improved efficiency. By default, files and subfolders inherit permissions from parent folders. Permissions can be explicitly modified at either the file or folder level to override inherited settings. In this case, the ACLs are a union of the parent ACLs and child ACLs.

Identity Crawling: Domain-wide access is supported using service account authentication. Google Drive supports nested groups, meaning that one group can be a member of another. The connector handles complex group structures by flattening group memberships and ensuring that permissions are applied correctly across all levels.

Change Management: ACL changes are automatically detected and processed during incremental synchronization.

Failure handling: The connector implements a fail-close approach, meaning that if there are permissions-related issues or API failures, a document is skipped from ingestion rather than being made publicly accessible.

Connecting Amazon Q Business to GoogleDrive using API

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- Google Drive configuration properties
- Google Drive JSON schema
- GoogleDrive JSON schema example
- GoogleDrive minimal configuration example

Google Drive configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`type`	The connector type. Must be `GOOGLEDRIVEV3` .	`string`	Yes
`connectionConfiguration`	Configuration information for the data source connection.	`object` This property has the following sub-properties: `secretArn` , `authType`.	Yes
`secretArn`	The Amazon Resource Name (ARN) of the AWS Secrets Manager secret that contains the Google Drive credentials.	`string`	Yes
`authType`	The authentication type. The valid value is: `SERVICE_ACCOUNT` .	`string`	Yes

Configuration	Description	Type	Required
`dataEntityConfiguration`	Configuration for which Google Drive entities to crawl.	`object` This property has the following sub-properties: `crawlMyDrive` , `crawlSharedWithMe` , `crawlSharedDrives` .	Yes
`crawlMyDrive`	Whether to crawl the user's personal drive. Default is `true`.	`boolean`	No
`crawlSharedWithMe`	Whether to crawl files shared with the user. Default is `true`.	`boolean`	No
`crawlSharedDrives`	Whether to crawl shared drives. Default is `true`.	`boolean`	No
`accessControlConfiguration`	Configuration for access control list (ACL) crawling.	`object` This property has the following sub-property: `crawlAcl`.	Yes
`crawlAcl`	Whether to crawl access control lists for documents.	`boolean`	No

Configuration	Description	Type	Required
`filterConfiguration`	Configuration for filtering which content to crawl.	`object` Contains various filtering options including shared drives, MIME types, and date ranges.	No
`maxFileSizeInMegaBytes`	Maximum file size to crawl in megabytes.	`string`	No
`exclusionSharedDriveIds`	Array of shared drive IDs to exclude from crawling. Maximum 1024 entries.	`array`	No
`inclusionSharedDriveIds`	Array of shared drive IDs to include in crawling. Maximum 1024 entries.	`array`	No
`exclusionMimeTypes`	Array of MIME types to exclude from crawling. Maximum 1024 entries.	`array`	No
`inclusionMimeTypes`	Array of MIME types to include in crawling. Maximum 1024 entries.	`array`	No

Configuration	Description	Type	Required
`modifiedDateBefore`	Only crawl files modified before this date. ISO 8601 format (e.g., 2024-12-31T23:59:59Z).	`string`	No
`modifiedDateAfter`	Only crawl files modified after this date. ISO 8601 format (e.g., 2024-01-01T00:00:00Z).	`string`	No
`crawlIdentities`	Whether to crawl user and group identities. Not supported in new.	`boolean`	No
`deletionProtectionConfiguration`	Configuration for deletion protection settings.	`object` This property has the following sub-properties: `enableDeletionProtection`, `deletionProtectionThreshold`.	No
`enableDeletionProtection`	Whether to enable deletion protection.	`boolean`	No

Configuration	Description	Type	Required
deletionProtectionThreshold	Threshold percentage for deletion protection.	string	No
version	Version of the connector configuration.	string	No
identityLoggingStatus	Status of identity logging. Valid values are ENABLED and DISABLED.	string	No

Google Drive JSON schema

The following is the Google Drive New JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["GOOGLEDRIVEV3"]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "secretArn": {
          "type": "string",
          "minLength": 20,
          "maxLength": 2048
        },
        "authType": {
          "type": "string",
          "enum": ["SERVICE_ACCOUNT"]
        }
      },
      "required": ["secretArn", "authType"]
    },
```

```
    "dataEntityConfiguration": {
      "type": "object",
      "properties": {
        "crawlMyDrive": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlSharedWithMe": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlSharedDrives": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        }
      }
    },
    "filterConfiguration": {
      "type": "object",
      "properties": {
        "maxFileSizeInMegaBytes": {
          "type": "string"
        },
```

```
        "exclusionSharedDriveIds": {
          "type": "array",
          "maxItems": 1024,
          "items": {
            "type": "string"
          }
        },
        "inclusionSharedDriveIds": {
          "type": "array",
          "maxItems": 1024,
          "items": {
            "type": "string"
          }
        },
        "exclusionMimeTypes": {
          "type": "array",
          "maxItems": 1024,
          "items": {
            "type": "string"
          }
        },
        "inclusionMimeTypes": {
          "type": "array",
          "maxItems": 1024,
          "items": {
            "type": "string"
          }
        },
        "modifiedDateBefore": {
          "type": "string",
          "format": "date-time",
          "description": "ISO 8601 date-time format (e.g., 2024-12-31T23:59:59Z)"
        },
        "modifiedDateAfter": {
          "type": "string",
          "format": "date-time",
          "description": "ISO 8601 date-time format (e.g., 2024-01-01T00:00:00Z)"
        }
      }
    },
    "accessControlConfiguration": {
      "type": "object",
      "properties": {
        "crawlAcl": {
```

```
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        }
      }
    },
    "crawlIdentities": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "deletionProtectionConfiguration": {
      "type": "object",
      "properties": {
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "deletionProtectionThreshold": {
          "type": "string"
        }
      }
    },
    "version": {
      "type": "string"
```

```
    },
    "identityLoggingStatus": {
      "type": "string",
      "enum": ["ENABLED", "DISABLED"]
    }
  },
  "required": ["type", "connectionConfiguration", "dataEntityConfiguration",
 "accessControlConfiguration"]
}
```

GoogleDrive JSON schema example

The following is the GoogleDrive New JSON schema example:

```
{
  "type": "GOOGLEDRIVEV3",
  "connectionConfiguration": {
    "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-google-drive-
secret",
    "authType": "SERVICE_ACCOUNT"
  },
  "dataEntityConfiguration": {
    "crawlMyDrive": true,
    "crawlSharedWithMe": true,
    "crawlSharedDrives": true
  },
  "filterConfiguration": {
    "maxFileSizeInMegaBytes": "50",
    "exclusionSharedDriveIds": ["SharedDrive1"],
    "inclusionSharedDriveIds": ["SharedDrive2"],
    "exclusionMimeTypes": ["application/vnd.google-apps.folder"],
    "inclusionMimeTypes": ["application/pdf", "application/vnd.google-apps.document"],
    "modifiedDateBefore": "2024-12-31T23:59:59Z",
    "modifiedDateAfter": "2024-01-01T00:00:00Z"
  },
  "accessControlConfiguration": {
    "crawlAcl": true
  },
  "crawlIdentities": true,
  "deletionProtectionConfiguration": {
    "enableDeletionProtection": false,
    "deletionProtectionThreshold": "10"
  },
  "version": "3.0.0",
```

```
  "identityLoggingStatus": "DISABLED"
}
```

GoogleDrive minimal configuration example

The following is the minimum required configuration for GoogleDrive New:

```
{
  "type": "GOOGLEDRIVEV3",
  "connectionConfiguration": {
    "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-google-drive-
secret",
    "authType": "SERVICE_ACCOUNT"
  },
  "dataEntityConfiguration": {
    "crawlMyDrive": true,
    "crawlSharedWithMe": false,
    "crawlSharedDrives": false
  },
  "accessControlConfiguration": {
    "crawlAcl": false
  }
}
```

Connecting Amazon Q Business to Google Drive using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- Google Drive New CloudFormation template

Google Drive New CloudFormation template

The following is the Google Drive New CloudFormation template. Copy and save this template to a file on your local drive.

For more information about CloudFormation templates, see Working with CloudFormation templates in the *CloudFormation User Guide*.

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Template to connect Google Drive New to Amazon Q Business",
  "Parameters": {
    "ApplicationId": {
      "Type": "String",
      "Description": "Amazon Q Business Application ID"
    },
    "IndexId": {
      "Type": "String",
      "Description": "Amazon Q Business Index ID"
    },
    "DataSourceName": {
      "Type": "String",
      "Description": "Name for the Google Drive data source"
    },
    "RoleArn": {
      "Type": "String",
      "Description": "IAM Role ARN for the data source"
    },
    "SecretArn": {
      "Type": "String",
      "Description": "AWS Secrets Manager ARN containing Google Drive credentials"
    }
  },
  "Resources": {
    "GoogleDriveV3DataSource": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": {"Ref": "ApplicationId"},
        "IndexId": {"Ref": "IndexId"},
        "DisplayName": {"Ref": "DataSourceName"},
        "RoleArn": {"Ref": "RoleArn"},
        "Configuration": {
          "type": "GOOGLEDRIVEV3",
          "connectionConfiguration": {
            "secretArn": {"Ref": "SecretArn"},
            "authType": "SERVICE_ACCOUNT"
          },
          "dataEntityConfiguration": {
```

```
            "crawlMyDrive": true,
            "crawlSharedWithMe": true,
            "crawlSharedDrives": false
          },
          "accessControlConfiguration": {
            "crawlAcl": true
          },
          "filterConfiguration": {
            "maxFileSizeInMegaBytes": "50"
          },
          "crawlIdentities": false,
          "deletionProtectionConfiguration": {
            "enableDeletionProtection": true,
            "deletionProtectionThreshold": "15"
          }
        }
      }
    }
  }
}
```

Connecting Google Drive to Amazon Q Business (Original)

> **Note**
>
> This documentation covers the original version of the Google Drive connector. For new implementations, we recommend using the New Google Drive connector which offers significantly improved performance. The original connector remains available for customers requiring specific features not yet supported in new.

Known limitations for the Amazon Q Business Google Drive connector

The Amazon Q Google Drive connector has the following known limitations:

- To make a document available to multiple users in Amazon Q Business, you need to explicitly add each user by their email address. Only documents with specific ACLs, including folder-level ACLs, will be available to your users for query responses within Amazon Q. The **Anyone with the link** feature is not supported.
- Custom field mapping is not available for Google Drive connector as the Google Drive UI does not support creating custom fields.

- Google Drive API does not support retrieving comments from a permanently deleted file. Comments are retrievable, however, for trashed files. When a file is trashed, the Amazon Q connector will delete comments from the Amazon Q index.
- Google Drive API does not return comments present in a .docx file.

Google Drive connector overview

The following table gives an overview of the Amazon Q Business Google Drive connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Google Service Account, OAuth 2.0 with Refresh Token Flow
	Authentication credentials	**Google service account** • Admin account email • Client email • Private key **OAuth 2.0 with Refresh Token Flow** • Client ID • Client secret • Refresh token **Important** Admin privileges required.
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes. Supported only with Google service account authentication.

Category	Feature	Support
	VPC	Yes
Crawl features	**Custom metadata**	No
	Entities	Yes. The following entities are supported: • Files • Comments See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports default field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include files based on file size • Include/exclude **Shared drives** • Include/exclude by mime types • Include/exclude attachments by file name, file type, and file path
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Google Drive

Before you begin, make sure that you have completed the following prerequisites.

In Google Drive, make sure you have:

- **Either** been granted access by a super admin role **or** are a user with administrative privileges. You do not need a super admin role for yourself if you have been granted access by a super admin role.

- Configured Google Drive Service Account connection credentials containing your admin account email, client email (service account email), and private key. See Google Cloud documentation on creating and deleting service account keys.
- Created a Google Cloud Service Account (an account with delegated authority to assume a user identity) with **Enable G Suite Domain-wide Delegation** activated for server-to-server authentication, and then generated a JSON private key using the account.

> **Note**
>
> The private key should be generated after the creation of the service account.

- Added Admin SDK API and Google Drive API in your user account.
- **Optional:** Configured Google Drive OAuth 2.0 connection credentials containing client ID, client secret, and refresh token as connection credentials for a specific user. You need this to crawl individual account data. See Google documentation on using OAuth 2.0 to access APIs.
- Added (or asked a user with a super admin role to add) the following OAuth scopes to your service account using a super admin role. These API scopes are needed to crawl all documents, and access control (ACL) information for all users in a Google Workspace domain:
  - https://www.googleapis.com/auth/drive.readonly—View and download all your Google Drive files
  - https://www.googleapis.com/auth/drive.metadata.readonly—View metadata for files in your Google Drive
  - https://www.googleapis.com/auth/admin.directory.group.readonly—Scope for only retrieving group, group alias, and member information. This is needed for the Amazon Q Identity Crawler.
  - https://www.googleapis.com/auth/admin.directory.user.readonly—Scope for only retrieving users or user aliases. This is needed for listing users in the Amazon Q Identity Crawler and for setting ACLs.
  - https://www.googleapis.com/auth/cloud-platform—Scope for generating access token for fetching content of large Google Drive files.
  - https://www.googleapis.com/auth/forms.body.readonly—Scope for fetching data from Google Forms.

  To support the Forms API, add the following additional scope:

  - https://www.googleapis.com/auth/forms.body.readonly

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Google Drive authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Google Drive using the console

The following procedure outlines how to connect Amazon Q Business to Google Drive using the AWS Management Console.

Connecting Amazon Q to Google Drive

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Google Drive** data source to your Amazon Q application.
5. Then, on the **Google Drive** data source page, enter the following information:
6. **Name and description**, do the following:
    - For **Data source name** – Name your data source for easy tracking.

> **Note**
>
> You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
8. For **Authentication** – Choose between **Google service account** and **OAuth 2.0 authentication**, based on your use case.
9. **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your GoogleDrive authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens.

   - If you choose **Existing**, select an existing secret for **Select secret**.

     If you choose **New**, enter the following information in the **New AWS Secrets Manager secret** section:

     i. **Secret name** – A name for your secret.

     ii. If you chose **Google service account**, enter the following information:

     - **Secret Name** – A name for your secret.
     - **Admin account email** – The email ID of the admin user (the email used by the Service Account User) in your Google service account configuration.
     - **Client email** – The email ID of the service account.
     - **Private Key** – The private key created in your service account.

     Then, choose **Save and add secret**.

iii. If you chose **OAuth 2.0 authentication**, enter the details of **Secret Name**, **Client ID**, **Client secret** and **Refresh token** that you created in your service account. Then, choose **Save and add secret**.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

    For more information, see IAM role.

12. In **Sync scope**, for **Sync contents** – Choose from the following options to select content to index:

> **Note**
>
> To further limit content to index, use **Entity regex patterns** in the **Additional configuration** section.

- **My Drive & Shared with me** – **My Drive** contains a user's personal folders and documents. **Shared with me** contains all the folders and documents that have been shared with the user. Select this option to index both.
- **Shared drives** – **Shared drives** are folders used to store, access, and share files with a team. Select this option to index these.

- **Comments** – Select this option to index file comments.

> **Note**
>
> If you add an inclusion pattern to include certain folder paths or files, you don't need to specify an exclude pattern to include the same folder paths or files.

13. For **Maximum file size** – You can specify the file size limit in GB for Amazon Q crawling. Amazon Q crawls only files within the defined size limit. The default file size is 50MB. The maximum file size limit is 10 GB. Files must be larger than 0 MB and no larger than 10 GB. You can go up to 10 GB (10240 MB) if you enable **Video files** in **Multi-media content** configuration, and up to 2 GB (2048 MB) if you enable **Audio files** in **Multi-media content configuration**.
14. In **Additional configuration - optional**, enter the following optional information:

    a. **User email** – Add the user email IDs whose drive files you want to include or exclude.

    b. **Shared drives** – The folders and files shared with a team. Add the shared drives that you want to include or exclude.

    c. **Mime types** – Add the MIME (Multipurpose Internet Mail Extensions) types that you want to include or exclude from your data sync.

    d. **Entity patterns** – Add regular expression patterns to include or exclude certain folders, files, and file types from **My drive**, **Shared with me**, and **Shared drives**. You can add up to 100 patterns.

    You can configure the Include/Exclude Regex patterns for File name, File type and File path.

    - **File name** - The name of the file to include/exclude. For example, to index a file with name 'Team roaster.txt', provide Team roaster.
    - **File type** - The type of the file to include/exclude. For example, .pdf .txt .docx
    - **File path** - The path of the file to include/exclude. For example, to index files only inside the folder 'Products list' of a drive, provide /Products list.

    e. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**. For more information, see Extracting semantic meaning from embedded images and visuals.

To extract audio transcriptions and video content, enable **Audio Files**. To extract video content, enable **Video files**. For more information, see Extracting semantic meaning from audio and video Content.

f. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

15. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

- **Full sync** – Sync all content regardless of the previous sync status.
- **New or modified content sync** – Sync only new and modified documents.
- **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

For more details, see Sync mode.

16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
18. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

> **Note**
>
> Documents shared to a specific company domain or with a permission set to **General access: Anyone with the link** must be accessed by at least one user before the documents become visible to users in search.

IAM role for Amazon Q Business Google Drive connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
```

```
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
```

```
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
```

```
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the Amazon Q Business Google Drive connector

The following table provides information about error codes you may see for the Google Drive connector and suggested resolutions.

Error code	Error message	Suggested resolution
GDL-5101	The authentication credentials in your data source configuration are invalid.	Verify your Google service account credentials or OAuth 2.0 tokens and try again.
GDL-5102	The authentication type in your data source configuration is missing or invalid.	Enter valid authentication type (Google Service Account or OAuth 2.0) and try again.
GDL-5103	Access denied to Google Drive API.	Ensure your service account has proper domain-wide delegation and API access enabled.
GDL-5104	Rate limit exceeded for Google Drive API.	Wait and retry. Consider reducing sync frequency if the issue persists.

Error code	Error message	Suggested resolution
GDL-5105	Invalid folder or file ID specified in filters.	Verify the folder or file IDs in your inclusion/exclusion filters are correct.

How Amazon Q Business connector crawls Google Drive ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

The Google Drive connector for Amazon Q Business crawls 2 primary content types: files and comments. It supports various file formats, including spreadsheets, presentations, images, audio/video files, and Google Docs™. Users can configure the connector to include or exclude comments.

Roles/permissions: The Google Drive connector translates Google Drive permissions into ACLs that are compatible with Amazon Q Business. There are four primary roles with permissions:

- Owner - Has full control.
- Editor - Can modify content, update metadata, and add or remove comments.
- Commenter - Can view content and add comments.
- Viewer - Has read-only access.

Permission Inheritance: The Google Drive connector is designed to detect and handle hierarchical content organization across My Drive and Shared Drives. By default, files and subfolders inherit permissions from parent folders. Comments inherit their permissions from the corresponding file. Permissions can be explicitly modified at either the file or folder level to override inherited settings. In this case, the ACLs are a union of the parent ACLs and child ACLs.

Identity Crawling: Individual user synchronization is supported using email addresses, and domain-wide access is supported using service account authentication. Google Drive supports nested groups, meaning that one group can be a member of another. The connector handles complex group structures by flattening group memberships and ensuring that permissions are applied correctly across all levels.

Change Management: ACL changes are supported in both Full Crawl and Incremental/Change Log modes

Failure handling: The connector implements a fail-close approach, meaning that if there are permissions-related issues or API failures, a document is skipped from ingestion rather than being made publicly accessible.

> **Note**
>
> The Google **Anyone with the link** feature is not supported by Amazon Q Business. To make a document available, you need to explicitly add users by their email address. Only documents with specific ACLs will be available to your users for query responses within Amazon Q.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Google Drive data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

The Amazon Q Google Drive connector supports the following entities and the associated reserved and custom attributes.

Files

Google Drive field name	Index field name	Description	Data type
authors	_authors	Default	String list
mimeType	gd_file_mime_type	Custom	String
size	gd_size	Custom	Long (numeric)

Google Drive field name	Index field name	Description	Data type
webViewLink	_source_uri	Default	String
createdAt	_created_at	Default	Date
modifiedAt	_last_updated_at	Default	Date

Comments

Google Drive field name	Index field name	Description	Data type
authors	_authors	Default	String list
commentType	gd_type	Custom	String
createdAt	_created_at	Default	Date
modifiedAt	_last_updated_at	Default	Date

Connecting Amazon Q Business to GoogleDrive using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- Google Drive configuration properties
- Google Drive JSON schema
- GoogleDrive JSON schema example

Google Drive configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the data source.	`object` This property has the following sub-property: `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source. This data source doesn't specify an endpoint. You choose your authentication type: `serviceAccount` and `OAuth2`. The connection information is included in an AWS Secrets Manager secret that you provide the `secretArn` .	`object` This property has the following sub-property: `authType`.	Yes
`authType`	Choose between `serviceAccount` and `OAuth2`, based on your use case.	`string`	Yes

Configuration	Description	Type	Required
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties: `file` and `comment`.	Yes
• `file` • `comment`	A list of objects that map the attributes or field names of your Google Drive to Amazon Q index field names.	`object` `object` These properties have the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName` • `dateFieldFormat`	No
`indexFieldName`	The field name of your Google Drive to Amazon Q index field names.	`string`	Yes
`indexFieldType`	The field type of your Google Drive to Amazon Q index field names.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes

Configuration	Description	Type	Required
`dataSourceFieldName`	The data source field name of your Google Drive to Amazon Q index field names.	`string`	Yes
`dateFieldFormat`	The date format of your Google Drive to Amazon Q index field names.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source	object This property has the following sub-properties. • isCrawlAcl • isCrawlMyDriveAndSharedWithMe • isCrawlSharedDrives • isCrawlComment • fieldForUserId • maxFileSizeInMegaBytes • excludeUserAccounts • excludeSharedDrives • excludeMimeTypes • includeUserAccounts • includeSharedDrives • includeMimeTypes	Yes

Configuration	Description	Type	Required
		• includeTargetAudienceGroup • inclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileTypePatterns • exclusionFileNamePatterns • inclusionFilePathFilter • exclusionFilePathFilter	

Configuration	Description	Type	Required
`isCrawlAcl`	Specify `true` to crawl access control informati on by default from documents. **Note** Amazon Q Business crawls ACL information to ensure responses are generated only from documents your end users have access to. See Authoriza tion for more details.	`boolean`	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No

Configuration	Description	Type	Required
maxFileSizeInMegaBytes	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50 MB. The maximum file size should be greater than 0MB and less than or equal to 50 MB. You can use up to 10 GB (10240 MB) if you set videoExtractionStatus to ENABLED in mediaExtractionConfiguration.videoExtractionConfiguration when using CreateDatasource or UpdateDatasource API. Otherwise, you can use up to 2 GB (2048 MB) if you set audioExtractionStatus to ENABLED in mediaExtr	string	No

Configuration	Description	Type	Required
	`actionConfiguration.audioExtractionConfiguration` when using the `CreateDatasource` or `UpdateDatasource` API.		
• `iscrawlComment`	`true` to index comments in your Google Drive data source.	`boolean`	No
• `isCrawlMyDriveAndSharedWithMe`	`true` to index MyDrive and Shared With Me Drives in your Google Drive data source.	`boolean`	No
• `isCrawlSharedDrives`	`true` to index Shared Drives in your Google Drive data source.	`boolean`	No

Configuration	Description	Type	Required
• excludeUserAccounts • excludeSharedDrives • excludeMimeTypes • exclusionFileTypePatterns • exclusionFileNamePatterns • exclusionFilePathFilter	A list of regular expression patterns to *exclude* specific files in your Google Drive data source. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an exclusion and inclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.	array	No

Configuration	Description	Type	Required
• includeUserAccounts • includeSharedDrives • includeMimeTypes • includeTargetAudienceGroup • inclusionFileTypePatterns • inclusionFileNamePatterns • inclusionFilePathFilter	A list of regular expression patterns to *include* specific files in your Google Drive data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.	array	No
type	The type of data source. We recommend GOOGLEDRIVEV2 as your data source type.	string Valid values are GOOGLEDRIVEV2 and GOOGLEDRIVE .	No

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to certain documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information,	`boolean`	Yes

Configuration	Description	Type	Required
	see Identity crawler.		
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	`string` You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required
secretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Google Drive.	string The secret must contain a JSON structure with the following keys: If using Google Service Account authentication: { "clientEmail": "user account email", "adminAccountEmail": "service account email", "privateKey": "private key" } If using OAuth 2.0 authentication: { "clientID": "OAuth client ID", "clientSecret": "client secret", "refreshToken": "refresh token" }	Yes

Configuration	Description	Type	Required
`version`	The version of this template that's currently supported.	`string`	No

Google Drive JSON schema

The following is the Google Drive JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["GOOGLEDRIVEV2", "GOOGLEDRIVE"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FORCED_FULL_CRAWL", "FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
```

```
          "properties": {
            "authType": {
              "type": "string",
              "enum": ["serviceAccount", "OAuth2"]
            }
          },
          "required": ["authType"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "file": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "STRING_LIST", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
```

```
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "comment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE", "STRING_LIST"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
```

```
      "properties": {
        "maxFileSizeInMegaBytes": {
          "type": "string"
        },
        "isCrawlComment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlMyDriveAndSharedWithMe": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlSharedDrives": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
```

```
            "enum": ["true", "false"]
          }
        ]
      },
      "fieldForUserId": {
        "type": "string"
      },
      "excludeUserAccounts": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "excludeSharedDrives": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "excludeMimeTypes": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "includeUserAccounts": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "includeSharedDrives": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "includeMimeTypes": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "includeTargetAudienceGroup": {
```

```
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFilePathFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFilePathFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
```

```
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      }
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "type",
    "syncMode",
    "secretArn",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

GoogleDrive JSON schema example

The following is the GoogleDrive JSON schema example:

```
{
  "type": "GOOGLEDRIVEV2",
  "syncMode": "FULL_CRAWL",
  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-google-drive-
secret",
  "enableIdentityCrawler": "true",
```

```
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "authType": "OAuth2"
    }
  },
  "repositoryConfigurations": {
    "file": {
      "fieldMappings": [
        {
          "indexFieldName": "file_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "comment": {
      "fieldMappings": [
        {
          "indexFieldName": "comment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    }
  },
  "additionalProperties": {
    "maxFileSizeInMegaBytes": "10240",
    "isCrawlComment": "true",
    "isCrawlMyDriveAndSharedWithMe": "true",
    "isCrawlSharedDrives": "false",
    "isCrawlAcl": "true",
    "fieldForUserId": "user@example.com",
    "excludeUserAccounts": ["user1@example.com", "user2@example.com"],
    "excludeSharedDrives": ["SharedDrive1"],
    "excludeMimeTypes": ["application/vnd.google-apps.folder"],
    "includeUserAccounts": ["user3@example.com"],
    "includeSharedDrives": ["SharedDrive2"],
    "includeMimeTypes": [
      "application/pdf",
      "application/vnd.google-apps.document"
    ],
    "includeTargetAudienceGroup": ["group1@example.com"],
```

```
    "inclusionFileTypePatterns": ["*.pdf"],
    "inclusionFileNamePatterns": ["*report*"],
    "exclusionFileTypePatterns": ["*.tmp"],
    "exclusionFileNamePatterns": ["*draft*"],
    "inclusionFilePathFilter": ["documents/"],
    "exclusionFilePathFilter": ["drafts/"],
    "enableDeletionProtection": "true",
    "deletionProtectionThreshold": "15"

  }
}
```

Connecting Amazon Q Business to Google Drive using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- Google Drive configuration properties
- Google Drive JSON schema for using the configuration property with AWS CloudFormation
- Google Drive YAML schema for using the configuration property with AWS CloudFormation

Google Drive configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the data source.	`object` This property has the following sub-property: `repositor`	Yes

Configuration	Description	Type	Required
		`yEndpoint Metadata .`	
`repositor yEndpoint Metadata`	The endpoint information for the data source. This data source doesn't specify an endpoint. You choose your authentication type: `serviceAccount` and `OAuth2`. The connection informati on is included in an AWS Secrets Manager secret that you provide the `secretArn .`	`object` This property has the following sub-prope rty: `authType`.	Yes
`authType`	Choose between `serviceAccount` and `OAuth2`, based on your use case.	`string`	Yes
`repositor yConfigur ations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties: `file` and `comment`.	Yes

Configuration	Description	Type	Required
• `file` • `comment`	A list of objects that map the attributes or field names of your Google Drive to Amazon Q index field names.	`object` `object` These properties have the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName` • `dateFieldFormat`	No
`indexFieldName`	The field name of your Google Drive to Amazon Q index field names.	`string`	Yes
`indexFieldType`	The field type of your Google Drive to Amazon Q index field names.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes
`dataSourceFieldName`	The data source field name of your Google Drive to Amazon Q index field names.	`string`	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The date format of your Google Drive to Amazon Q index field names.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source	object This property has the following sub-properties. • isCrawlAcl • isCrawlMyDriveAndSharedWithMe • isCrawlSharedDrives • isCrawlComment • fieldForUserId • maxFileSizeInMegaBytes • excludeUserAccounts • excludeSharedDrives • excludeMimeTypes • includeUserAccounts • includeSharedDrives • includeMimeTypes	Yes

Configuration	Description	Type	Required
		• includeTargetAudienceGroup • inclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileTypePatterns • exclusionFileNamePatterns • inclusionFilePathFilter • exclusionFilePathFilter	

Configuration	Description	Type	Required
`isCrawlAcl`	Specify `true` to crawl access control informati on by default from documents. **Note** Amazon Q Business crawls ACL information to ensure responses are generated only from documents your end users have access to. See Authoriza tion for more details.	`boolean`	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No

Configuration	Description	Type	Required
maxFileSizeInMegaBytes	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50 MB. The maximum file size should be greater than 0MB and less than or equal to 50 MB. You can use up to 10 GB (10240 MB) if you set videoExtractionStatus to ENABLED in mediaExtractionConfiguration.videoExtractionConfiguration when using CreateDatasource or UpdateDatasource API. Otherwise, you can use up to 2 GB (2048 MB) if you set audioExtractionStatus to ENABLED in mediaExtr	string	No

Configuration	Description	Type	Required
	`actionConfiguration.audioExtractionConfiguration` when using the `CreateDatasource` or `UpdateDatasource` API.		
• `iscrawlComment`	`true` to index comments in your Google Drive data source.	`boolean`	No
• `isCrawlMyDriveAndSharedWithMe`	`true` to index MyDrive and Shared With Me Drives in your Google Drive data source.	`boolean`	No
• `isCrawlSharedDrives`	`true` to index Shared Drives in your Google Drive data source.	`boolean`	No

Configuration	Description	Type	Required
• excludeUserAccounts • excludeSharedDrives • excludeMimeTypes • exclusionFileTypePatterns • exclusionFileNamePatterns • exclusionFilePathFilter	A list of regular expression patterns to *exclude* specific files in your Google Drive data source. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an exclusion and inclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.	array	No

Configuration	Description	Type	Required
• includeUserAccounts • includeSharedDrives • includeMimeTypes • includeTargetAudienceGroup • inclusionFileTypePatterns • inclusionFileNamePatterns • inclusionFilePathFilter	A list of regular expression patterns to *include* specific files in your Google Drive data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.	array	No
type	The type of data source. We recommend GOOGLEDRIVEV2 as your data source type.	string Valid values are GOOGLEDRIVEV2 and GOOGLEDRIVE .	No

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to certain documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information,	`boolean`	Yes

Configuration	Description	Type	Required
	see Identity crawler.		
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required
secretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Google Drive.	string The secret must contain a JSON structure with the following keys: If using Google Service Account authentication: { "clientEmail": "user account email", "adminAccountEmail": "service account email", "privateKey": "private key" } If using OAuth 2.0 authentication: { "clientID": "OAuth client ID", "clientSecret": "client secret", "refreshToken": "refresh token" }	Yes

Configuration	Description	Type	Required
`version`	The version of this template that's currently supported.	`string`	No

Google Drive JSON schema for using the configuration property with AWS CloudFormation

The following is the Google Drive JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- Google Drive JSON schema for using the configuration property with AWS CloudFormation
- Google Drive JSON schema example for using the configuration property with AWS CloudFormation

Google Drive JSON schema for using the configuration property with AWS CloudFormation

The following is the Google Drive JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["GOOGLEDRIVEV2", "GOOGLEDRIVE"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FORCED_FULL_CRAWL", "FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
```

```
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "authType": {
              "type": "string",
              "enum": ["serviceAccount", "OAuth2"]
            }
          },
          "required": ["authType"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "file": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "STRING_LIST", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
```

```
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "comment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "STRING_LIST"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
```

```
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "isCrawlComment": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlMyDriveAndSharedWithMe": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlSharedDrives": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
```

```
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlAcl": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "fieldForUserId": {
        "type": "string"
      },
      "excludeUserAccounts": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "excludeSharedDrives": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "excludeMimeTypes": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "includeUserAccounts": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "includeSharedDrives": {
```

```
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "includeMimeTypes": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "includeTargetAudienceGroup": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFilePathFilter": {
          "type": "array",
          "items": {
```

```
            "type": "string"
          }
        },
        "exclusionFilePathFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      }
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "type",
    "syncMode",
    "secretArn",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
```

```
}
```

Google Drive JSON schema example for using the configuration property with AWS CloudFormation

The following is the Google Drive JSON schema example for the configuration property for CloudFormation

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation GOOGLEDRIVE Data Source Template",
  "Resources": {
    "DataSourceGoogleDrive": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MyGoogleDriveDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "GOOGLEDRIVEV2",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-google-
drive-secret",
          "enableIdentityCrawler": "true",
          "connectionConfiguration": {
            "repositoryEndpointMetadata": {
              "authType": "OAuth2"
            }
          },
          "repositoryConfigurations": {
            "file": {
              "fieldMappings": [
                {
                  "indexFieldName": "file_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
            },
            "comment": {
              "fieldMappings": [
```

```
                {
                  "indexFieldName": "comment_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
            }
          },
          "additionalProperties": {
            "maxFileSizeInMegaBytes": "50",
            "isCrawlComment": "true",
            "isCrawlMyDriveAndSharedWithMe": "true",
            "isCrawlSharedDrives": "false",
            "isCrawlAcl": "true",
            "fieldForUserId": "user@example.com",
            "excludeUserAccounts": ["user1@example.com", "user2@example.com"],
            "excludeSharedDrives": ["SharedDrive1"],
            "excludeMimeTypes": ["application/vnd.google-apps.folder"],
            "includeUserAccounts": ["user3@example.com"],
            "includeSharedDrives": ["SharedDrive2"],
            "includeMimeTypes": [
              "application/pdf",
              "application/vnd.google-apps.document"
            ],
            "includeTargetAudienceGroup": ["group1@example.com"],
            "inclusionFileTypePatterns": ["*.pdf"],
            "inclusionFileNamePatterns": ["*report*"],
            "exclusionFileTypePatterns": ["*.tmp"],
            "exclusionFileNamePatterns": ["*draft*"],
            "inclusionFilePathFilter": ["documents/"],
            "exclusionFilePathFilter": ["drafts/"],
            "enableDeletionProtection": "true",
            "deletionProtectionThreshold": "15"
          }
        }
      }
    }
  }
}
```

Google Drive YAML schema for using the configuration property with AWS CloudFormation

The following is the Google Drive YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- Google Drive YAML schema for using the configuration property with AWS CloudFormation
- Google Drive YAML schema example for using the configuration property with AWS CloudFormation

Google Drive YAML schema for using the configuration property with AWS CloudFormation

The following is the Google Drive YAML schema for the configuration property for CloudFormation.

```
type: object
properties:
  type:
    type: string
    enum:
      - GOOGLEDRIVEV2
      - GOOGLEDRIVE
  syncMode:
    type: string
    enum:
      - FORCED_FULL_CRAWL
      - FULL_CRAWL
      - CHANGE_LOG
  secretArn:
    type: string
    minLength: 20
    maxLength: 2048
  enableIdentityCrawler:
    anyOf:
      - type: boolean
      - type: string
        enum:
          - true
          - false
  connectionConfiguration:
    type: object
    properties:
      repositoryEndpointMetadata:
```

```
        type: object
        properties:
          authType:
            type: string
            enum:
              - serviceAccount
              - OAuth2
        required:
          - authType
    required:
      - repositoryEndpointMetadata
  repositoryConfigurations:
    type: object
    properties:
      file:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - DATE
                    - STRING_LIST
                    - LONG
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      comment:
        type: object
```

```
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - DATE
                    - STRING_LIST
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
  additionalProperties:
    type: object
    properties:
      maxFileSizeInMegaBytes:
        type: string
      isCrawlComment:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      isCrawlMyDriveAndSharedWithMe:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
```

```
      isCrawlSharedDrives:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      isCrawlAcl:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      fieldForUserId:
        type: string
      excludeUserAccounts:
        type: array
        items:
          type: string
      excludeSharedDrives:
        type: array
        items:
          type: string
      excludeMimeTypes:
        type: array
        items:
          type: string
      includeUserAccounts:
        type: array
        items:
          type: string
      includeSharedDrives:
        type: array
        items:
          type: string
      includeMimeTypes:
        type: array
        items:
          type: string
      includeTargetAudienceGroup:
        type: array
        items:
          type: string
```

```
      inclusionFileTypePatterns:
        type: array
        items:
          type: string
      inclusionFileNamePatterns:
        type: array
        items:
          type: string
      exclusionFileTypePatterns:
        type: array
        items:
          type: string
      exclusionFileNamePatterns:
        type: array
        items:
          type: string
      inclusionFilePathFilter:
        type: array
        items:
          type: string
      exclusionFilePathFilter:
        type: array
        items:
          type: string
      enableDeletionProtection:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
        default: false
      deletionProtectionThreshold:
        type: string
        default: "15"
  version:
    type: string
    anyOf:
      - pattern: 1.0.0
required:
  - type
  - syncMode
  - secretArn
  - connectionConfiguration
```

```
  - repositoryConfigurations
  - additionalProperties
```

Google Drive YAML schema example for using the configuration property with AWS CloudFormation

The following is the Google Drive YAML example for the Configuration property for CloudFormation:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: CloudFormation GOOGLEDRIVE Data Source Template
Resources:
  DataSourceGoogleDrive:
    Type: AWS::QBusiness::DataSource
    Properties:
      ApplicationId: app12345-1234-1234-1234-123456789012
      IndexId: indx1234-1234-1234-1234-123456789012
      DisplayName: MyGoogleDriveDataSource
      RoleArn: arn:aws:iam::123456789012:role/qbusiness-data-source-role
      Configuration:
        type: GOOGLEDRIVEV2
        syncMode: FULL_CRAWL
        secretArn: arn:aws:secretsmanager:us-west-2:123456789012:secret:my-google-
drive-secret
        enableIdentityCrawler: "true"
        connectionConfiguration:
          repositoryEndpointMetadata:
            authType: OAuth2
        repositoryConfigurations:
          file:
            fieldMappings:
              - indexFieldName: file_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
          comment:
            fieldMappings:
              - indexFieldName: comment_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
        additionalProperties:
          maxFileSizeInMegaBytes: "50"
```

```
        isCrawlComment: "true"
        isCrawlMyDriveAndSharedWithMe: "true"
        isCrawlSharedDrives: "false"
        isCrawlAcl: "true"
        fieldForUserId: user@example.com
        excludeUserAccounts:
          - user1@example.com
          - user2@example.com
        excludeSharedDrives:
          - SharedDrive1
        excludeMimeTypes:
          - application/vnd.google-apps.folder
        includeUserAccounts:
          - user3@example.com
        includeSharedDrives:
          - SharedDrive2
        includeMimeTypes:
          - application/pdf
          - application/vnd.google-apps.document
        includeTargetAudienceGroup:
          - group1@example.com
        inclusionFileTypePatterns:
          - "*.pdf"
        inclusionFileNamePatterns:
          - "*report*"
        exclusionFileTypePatterns:
          - "*.tmp"
        exclusionFileNamePatterns:
          - "*draft*"
        inclusionFilePathFilter:
          - documents/
        exclusionFilePathFilter:
          - drafts/
        enableDeletionProtection: "true"
        deletionProtectionThreshold: "15"
```

Connecting Jira to Amazon Q Business

Jira is a project management tool for software development, product management, and bug tracking. You can connect your Jira instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the Amazon Q Jira connector
- Jira connector overview
- Prerequisites for connecting Amazon Q Business to Jira
- Setting up Jira for connecting to Amazon Q Business
- Connecting Amazon Q Business to Jira using the console
- Connecting Amazon Q Business to Jira using APIs
- Connecting Amazon Q Business to Jira using AWS CloudFormation
- How Amazon Q Business connector crawls Jira ACLs
- Jira data source connector field mappings
- IAM role for Amazon Q Business Jira connector
- Understand error codes in the Amazon Q Business Jira connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Amazon Q Jira connector

The Amazon Q Jira connector has the following known limitations:

- Deleted Issues in Jira are not available through Jira APIs. The Amazon Q Jira connector won't be able to fetch information about deleted Jira issues during incremental syncs.
- Private and Empty projects aren't crawled by the Amazon Q Jira connector.

Jira connector overview

The following table gives an overview of the Amazon Q Business Jira connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic, Basic, OAuth 2.0 with Refresh Token Flow
	Authentication credentials	For Basic authentication • Jira URL • Jira username • Password (Jira site token) For OAuth 2.0 authentication with Refresh Token Flow • App key • App secret • Access token • Refresh token **Note** Access and refresh tokens expire in 1 hour. For information on regenerating tokens, see Atlassian Developer Documentation.
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	No
	VPC	Yes
Crawl features	**Custom objects**	Yes
	Custom metadata	Yes

Category	Feature	Support
	Entities	Yes. The following entities are supported: • Projects • Issues • Comments • Attachments • Worklogs See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include specific projects • Include/exclude statuses • Include/exclude comments • Include/exclude attachments • Include/exclude worklogs • Include/exclude bugs • Include/exclude epic • Include/exclude story • Include/exclude task • Include/exclude by file name • Include/exclude by file type • Include/exclude by file path
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Jira

Before you begin, make sure that you have completed the following prerequisites.

In Jira, make sure you have:

- Created Jira API token authentication credentials that include a Jira ID (email ID with domain) and a Jira credential (Jira API token). See the Atlassian documentation for information about managing API tokens.
- Noted the Jira account URL from your Jira account settings. For example, *`https://company.atlassian.net/`*.
- Noted your Jira project key ID from your Jira project settings if you want to crawl only specific Jira projects.
- If you want to have Amazon Q automatically rotate your secret, ensure that your IAM role includes the `secretsmanager:PutSecretValue` and `secretsmanager:UpdateSecret` permissions.

If you have company-managed Jira projects, you need to perform the following:

- **Administer Jira Permissions**: The service account - the user configuring the Amazon Q Business integration - must have **Administer Jira** permissions. These permissions are required to read and interpret the permission schemes of company-managed projects to build appropriate Access Control Lists (ACLs). To assign this permission, go to the Settings icon in Jira, then navigate to **System > Global Permissions**. Add the *Administer Jira* permission to the service account.
- **Email Visibility Settings**: Jira must provide access to the email address of the users for Amazon Q Business to correctly validate document-level permissions. To enable this, update profile settings by navigating to **Profile Picture** → **Manage Account > Privacy**, and setting **Email Visibility** to Anyone. This is a requirement due to limitations in Jira's API that impact integrations with external tools such as Amazon Q Business.
- **User and Project-Level Permissions**: The admin user associated with the integration must have at least **Browse Projects** permission in Jira. This can be granted directly or indirectly through a group, project role, or any other applicable configuration. To verify permissions, navigate to the specific Jira project, go to **Project Settings > Permissions**, and confirm that the admin user **Browse Projects** permission. To validate permissions, use the **Permission Helper**. Enter the user alias and select **Browse Projects** permission to check access.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Jira authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

> **Note**
>
> For more information on connecting Jira to Amazon Q Business, see Improve the productivity of your customer support and project management teams using Amazon Q Business and Atlassian Jira in the *AWS Machine Learning Blog*.

Setting up Jira for connecting to Amazon Q Business

Before you connect Jira to Amazon Q Business, you need to create and retrieve the Jira credentials you will use to connect Jira to Amazon Q. You will also need to add any permissions needed by Jira to connect to Amazon Q.

The following sections give you an overview of how to configure Jira to connect to Amazon Q using either basic authentication or OAuth 2.0 authentication.

Topics

- Basic authentication
- OAuth 2.0 authentication
- How Amazon Q works with Jira access and refresh tokens

- Checking Jira connectivity

Basic authentication

You can connect Amazon Q to Jira using basic authentication credentials. The following procedure gives you an overview of how to configure Jira to connect to Amazon Q using basic authentication.

Configuring Jira basic authentication for Amazon Q

1. Log in to your account from Jira. Note the username you logged in with. You will need this later to connect to Amazon Q.
2. From your Jira home page, copy the Jira URL from your Jira browser URL. For example: *https://example.atlassian.net*. You will need this later to connect to Amazon Q.
3. Then, go to Security page in Jira.
4. From the **API tokens** page, select **Create API token**.
5. In the **Create an API token** dialog box that opens, for **Label**, add a name for your API token. Then, select **Create**.
6. From the **Your new API token** dialog box, copy the API token and save it in a text editor of your choice. You can't retrieve the API token once you close the dialog box.
7. Select **Close**.

You now have the username, Jira URL, and Jira API token you need to connect to Amazon Q with basic authentication.

For more information, see Manage API tokens for your Atlassian account in Atlassian Support.

OAuth 2.0 authentication

You can connect Amazon Q to Jira using OAuth 2.0 authentication credentials. The following procedures give you an overview of how to configure Jira to connect to Amazon Q using OAuth 2.0 authentication.

Steps to configure Jira OAuth 2.0 authentication

- Step 1: Retrieving username and Jira URL
- Step 2: Configuring an OAuth 2.0 app integration
- Step 3: Retrieving Jira client ID and client Secret

- Step 4: Generating a Jira access token
- Step 5: Generating a Jira refresh token
- Step 6: Generating a new Jira access token using a refresh token

Step 1: Retrieving username and Jira URL

To connect Jira to Amazon Q, you need your Jira username and your Jira URL. The following procedure shows you how to retrieve these.

Retrieving username and Jira URL

1. Log in to your account from the Jira. Note the username you logged in with. You will need this later to connect to Amazon Q.
2. From your Jira home page, note your Jira URL from your Jira browser URL. For example: *`https://example.atlassian.net`*. You will need this later to both configure your OAuth 2.0 token and connect to Amazon Q.

Step 2: Configuring an OAuth 2.0 app integration

To connect Jira to Amazon Q using OAuth 2.0 authentication, you need to create a Jira OAuth 2.0 app with the necessary permissions. The following procedure shows you how to create this.

Configuring an OAuth 2.0 app integration

1. Log in to your account from the Atlassian Developer page.
2. Select the profile icon from the top-right corner. Then, from the dropdown menu that opens, select **Developer Console**.
3. From the **Welcome** page, select **Create** and then select **OAuth 2.0 integration**.
4. On the **Create a new OAuth 2.0 (3LO) integration** page, for **Name**, enter a name for the OAuth 2.0 application you are creating. Then, select the **I agree to be bound by Atlassian's developer terms** checkbox, and select **Create**.

   The console will display a summary page outlining the details of the OAuth 2.0 app created.
5. From the left navigation menu, choose **Authorization**.
6. From the **Authorization** page, choose **Add** to add **OAuth 2.0 (3LO)** to your app.
7. On the **OAuth 2.0 authorization code grants (3LO) for apps**, enter the Jira URL you copied as the **Callback URL** and then choose **Save changes**.

8. From the **Authorization URL generator** section that appears, choose **Add APIs** to add APIs to your app. This will redirect you to the **Permissions** page.
9. On the **Permissions** page, for **Scopes**, navigate to **User Identity API**. Select **Add**, and then select **Configure**.
10. On the **User Identity API** page, choose **Edit Scopes**, and the add the following `read` scopes:

    - **`read:me`** – View active user profile
    - **`read:account`** – View user profiles

    Then, select **Save**.
11. Return to the **Permissions** page. From **Scopes**, navigate to **Jira API**. Select **Add**, and then select **Configure**.
12. On the **Jira API** page, you need to add scopes from both the Classic scopes and Granular scopes sections.

    Choose **Edit Scopes**, and add the following scopes:

    In the Classic scopes section, add:

    - **`read:jira-user`** – View active user profiles
    - **`read:jira-work`** – View Jira issue data
    - **`manage:jira-configuration`** – Manage Jira global settings

    In the Granular scopes section, add:

    - **`read:application-role:jira`** – View application roles

    Select **Save**.

For more information, see Implementing OAuth 2.0 (3LO) and Determining the scopes required for an operation in Atlassian Developer.

Step 3: Retrieving Jira client ID and client Secret

To connect Jira to Amazon Q using OAuth 2.0 authentication, you need to provide a Jira client ID and client secret. The following procedure shows you how to retrieve these.

> **Note**
>
> You must create an OAuth 2.0 app before you can retrieve the client ID and client secret. See Configuring an OAuth 2.0 app integration for more details.

Retrieving Jira client ID and client secret

- From the left navigation menu, choose **Settings**. Then, scroll down to **Authentication details** section and copy and save the following in a text editor of your choice:
  - Client ID – You will enter this as **App key** in the Amazon Q console.
  - Client Secret – You will enter this as **App secret** in the Amazon Q console.

  You will need these to generate your Jira OAuth 2.0 token and also to connect Amazon Q to Jira.

For more information, see Implementing OAuth 2.0 (3LO) and Determining the scopes required for an operation in Atlassian Developer.

Step 4: Generating a Jira access token

To connect Jira to Amazon Q, you need to generate an access token. The following procedure outlines how to generate an access token in Jira.

Generating your Jira access token

1. Log in to your account from the Atlassian Developer page.
2. Open the OAuth 2.0 app you want to generate a refresh token for.
3. From the left navigation menu, choose **Authorization** again. Then, for **OAuth 2.0 (3LO)**, choose **Configure**.
4. From the **Authorization** page, from **Authorization URL generator**, from **Granular Jira API authorization URL**, copy the URL and save it in a text editor of your choice.

   The URL is of the following format:

   ```
   https://auth.atlassian.com/authorize?
   audience=api.atlassian.com
   ```

```
&client_id=YOUR_CLIENT_ID
&scope=REQUESTED_SCOPE%20REQUESTED_SCOPE_TWO
&redirect_uri=https://YOUR_APP_CALLBACK_URL
&state=YOUR_USER_BOUND_VALUE
&response_type=code
&prompt=consent
```

5. In the saved authorization URL, update the `state=${YOUR_USER_BOUND_VALUE}` parameter value to any text of your choice. For example, `state=sample_text`.

   For more information, see What is the state parameter used for? in Atlassian Support.

6. Open a web browser of your choice. Then, paste the authorization URL you copied into the browser URL. On the page that opens up, make sure everything is correct and then select **Accept**.

   You will be returned to your Jira home page.

7. Copy the URL of the Jira home page and save it in a text editor of your choice. The URL contains the authorization code for your application. You will need this code to generate your Jira access token. The whole section after `code=` is the authorization code.

8. Navigate to Postman.

   If you don't have Postman, you can also choose to use cURL to generate a Jira access token. Use the following cURL command to do so:

```
curl --location 'https://auth.atlassian.com/oauth/token' \
--header 'Content-Type: application/json' \
--data '{"grant_type": "authorization_code",
"client_id": "YOUR_CLIENT_ID",
"client_secret": "YOUR_CLIENT_SECRET",
"code": "AUTHORIZATION_CODE",
"redirect_uri": "YOUR_CALLBACK_URL"}'
```

9. On the Postman home page, select POST as the method, and then enter the following URL in the **Enter URL or paste text** box: `https://auth.atlassian.com/oauth/token`.

10. Then, select **Body** from the menu, and select **raw JSON**.

11. In the text box, enter the following code extract, replacing the fields with your credential values:

```
{"grant_type": "authorization_code",
"client_id": "YOUR_CLIENT_ID",
```

```
"client_secret": "YOUR_CLIENT_SECRET",
"code": "YOUR_AUTHORIZATION_CODE",
"redirect_uri": "https://YOUR_APP_CALLBACK_URL"}
```

12. Then, select **Send**. If everything is configured correctly, Postman will return an `access-token`. Copy the access token and save it using a text editor of your choice. You will need it to connect Jira to Amazon Q.

For more information, see Implementing OAuth 2.0 (3LO) in Atlassian Developer.

Step 5: Generating a Jira refresh token

The access token you use to connect Jira to Amazon Q using OAuth 2.0 authentication expires after 1 hour. When it does, you can either repeat the whole authorization process and generate a new access token. Or, you can choose to generate a refresh token. You can use the refresh token to regenerate a new access token when an existing access token expires.

To do this, you add a `%20offline_access` parameter to the end of the `scope` value in the authorization URL you used to generate your access token. The following procedure shows you how to generate a refresh token.

Generating an Jira refresh token

1. Log in to your account from the Atlassian Developer page.
2. Open the OAuth 2.0 app you want to generate a refresh token for.
3. From the left navigation menu, choose **Authorization** again. Then, for **OAuth 2.0 (3LO)**, choose **Configure**.
4. From the **Authorization** page, from **Authorization URL generator**, from **Granular Jira API authorization URL**, copy the URL and save it in a text editor of your choice.
5. In the saved authorization URL, update the `state=${YOUR_USER_BOUND_VALUE}` parameter value to any text of your choice. For example, `state=sample_text`.

   For more information, see What is the state parameter used for? in Atlassian Support.
6. Then, add the following text at the end of the `scope` value in your authorization URL: `%20offline_access` and copy it. For example:

```
https://auth.atlassian.com/authorize?
```

```
audience=api.atlassian.com
&client_id=YOUR_CLIENT_ID
&scope=REQUESTED_SCOPE%20REQUESTED_SCOPE_TWO%20offline_access
&redirect_uri=https://YOUR_APP_CALLBACK_URL
&state=YOUR_USER_BOUND_VALUE
&response_type=code
&prompt=consent
```

7. Open a web browser of your choice and paste the modified authorization URL you copied into the browser URL. On the page that opens up, make sure everything is correct and then select **Accept**.

   You will be returned to the Jira console.

8. Copy the URL of the Jira home page and save it in a text editor of your choice. The URL contains the authorization code for your application. You will need this code to generate your Jira refresh token. The whole section after `code=` is the authorization code.

9. Navigate to Postman.

   If you don't have Postman, you can also choose to use cURL to generate a Jira access token. Use the following cURL command to do so:

```
curl --location 'https://auth.atlassian.com/oauth/token' \
--header 'Content-Type: application/json' \
--data '{"grant_type": "authorization_code",
"client_id": "YOUR CLIENT ID",
"client_secret": "YOUR CLIENT SECRET",
"code": "AUTHORIZATION CODE",
"redirect_uri": "YOUR CALLBACK URL"}'
```

10. On the Postman home page, select POST as the method, and then enter the following URL in the **Enter URL or paste text** box: `https://auth.atlassian.com/oauth/token`.

11. Then, select **Body** from the menu, and select **raw JSON**.

12. In the text box, enter the following code extract, replacing the fields with your credential values:

```
{"grant_type": "authorization_code",
"client_id": "YOUR_CLIENT_ID",
"client_secret": "YOUR_CLIENT_SECRET",
"code": "YOUR_AUTHORIZATION_CODE",
"redirect_uri": "https://YOUR_APP_CALLBACK_URL"}
```

13. Then, select **Send**. If everything is configured correctly, Postman will return an `refresh-token`.

    Copy the refresh token and save it using a text editor of your choice. You will need it to connect Jira to Amazon Q.

For more information, see Implementing a Refresh Token Flow in Atlassian Developer.

Step 6: Generating a new Jira access token using a refresh token

You can use the refresh token you generated to create a new access token-refresh token pair when an existing access token expires. The following procedure shows you how to generate a refresh token.

Generating an Jira access token-refresh token pair

1. Copy the refresh token you generated following the steps in Step 5: Generating a Jira refresh token.
2. Navigate to Postman.

   If you don't have Postman, you can also choose to use cURL to generate a new Jira access token. Use the following cURL command to do so:

   ```
   curl --location 'https://auth.atlassian.com/oauth/token' \
   --header 'Content-Type: application/json' \
   --data '{"grant_type": "refresh_token",
   "client_id": "YOUR_CLIENT_ID",
   "client_secret": "YOUR_CLIENT_SECRET",
   "refresh_token": "YOUR_REFRESH_TOKEN"}'
   ```

3. On the Postman home page, select POST as the method, and then enter the following URL in the **Enter URL or paste text** box: `https://auth.atlassian.com/oauth/token`.
4. Then, select **Body** from the menu, and select **raw JSON**.
5. In the text box, enter the following code extract, replacing the fields with your credential values:

   ```
   {"grant_type": "refresh_token",
   "client_id": "YOUR_CLIENT_ID",
   ```

```
"client_secret": "YOUR_CLIENT_SECRET",
"refresh_token": "YOUR REFRESH TOKEN"}
```

6. Then, select **Send**. If everything is configured correctly, Postman will return a new access token-refresh token pair in the following format:

```
{
"access_token": "string,
"expires_in": "expiry time of access_token in second",
"scope": "string",
"refresh_token": "string"
}
```

For more information, see Implementing a Refresh Token Flow and How do I get a new access token, if my access token expires or is revoked? in Atlassian Developer.

How Amazon Q works with Jira access and refresh tokens

The following are important points to note about using Jira access and refresh tokens with Amazon Q:

- If a Jira access token-refresh token pair you use to connect to Amazon Q are expired or invalid, the Amazon Q sync process fails. If this happens, you need to generate and provide a new pair of tokens.
- If your access token is valid but you have an invalid refresh token, Amazon Q will sync data until the access token expires (up to 1 hour). After the access token expires, you won't be able to re-generate an access token-refresh token pair using the expired refresh token. When both access token and refresh token expire, the Amazon Q Jira data source connector stops syncing.
- If an access token expires during the Jira connector sync process, the connector internally regenerates a new pair of tokens using the existing refresh token (if the provided refresh token is valid). After regenerating the new pair of tokens, the old pair is invalidated by Jira and can't be re-used. To sync documents again after the connector auto-regenerates tokens, you must provide a new access token-refresh token pair.
- If you use OAuth, select **Rotate secret** if you want Amazon Q to rotate the secret automatically so that you don’t have to manually update the secret every time before you sync.
- As a best practice, use Jira OAuth and the **Rotate secret** feature for the Amazon Q connector.

Checking Jira connectivity

Before you sync your Jira data source connector after configuring it, we recommend you check the connection between Amazon Q Business and Jira. The following are the cURL commands you need to check Jira connectivity.

Topics

- Checking basic authentication connectivity

Checking basic authentication connectivity

To check connectivity for a Jira data source connector using basic authentication, use the following cURL command:

```
curl --location 'https://<jira-url>/wiki/rest/api/user/current'
--header 'Authorization: Basic <base64(email:api_token)>'
```

If your data source is connected as expected, the JSON response should resemble the following:

```
{
    "type": "known",
    "accountId": "accountId",
    "accountType": "atlassian",
    "email": "email",
    "publicName": "Administrator",
    "profilePicture": {
        "path": "/wiki/aa-avatar/<accountId>",
        "width": 48,
        "height": 48,
        "isDefault": false
    },
    "displayName": "Administrator",
    "isExternalCollaborator": false,
    "_expandable": {
        "operations": "",
        "personalSpace": ""
    },
    "_links": {
        "self": "https://<host_url>/wiki/rest/api/user?accountId=<accountId>",
        "base": "https://<host_url>/wiki",
        "context": "/wiki"
    }
```

```
}
```

If your Jira connector is not connected correctly, you will see the following error:

- CNF-5123: The profile value is invalid. Try again after sometime.

To troubleshoot the issue, check your Jira URL and make sure it's correct.

Connecting Amazon Q Business to Jira using the console

The following procedure outlines how to connect Amazon Q Business to Jira using the AWS Management Console.

Connecting Amazon Q to Jira

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Jira** data source to your Amazon Q application.
5. Then, on the **Jira** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. **Source** – Enter your **Jira URL**. For example: *`https://company.atlassian.net/`*.
8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

    a. **Secret name** – A name for your secret.

    b. **Jira ID** – Your Jira email id, with domain. For example, *marymajor@gmail.com*.

    c. **Password/Token** – Your Jira API token.

    For more information on creating a Jira token, see API Tokens.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.

12. In **Sync scope**, enter the following information:

    a. Choose to either sync **All projects** or sync **Only specific projects**. If you choose to sync **Only specific projects**, enter the **Jira Project Key ID**.

    b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

    c. **Additional configuration – *optional*** – Choose from the following options to limit the scope for content to be indexed. If no filters are specified, all content will be synced by default.

- **Statuses** – Add status values to index.
- **Additional elements** – Choose whether to index **Comments**, **Attachments**, or **Worklogs**.
- **Issue types** – Optionally choose specific issue types to index. If no issue types are selected, all issue types will be indexed by default.
- **Regex patterns** – Add regex patterns to include or exclude file names, file types, or file paths. You can have a total of 100 patterns.

d. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

To extract audio transcriptions and video content, enable processing for the following file types:

e. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

13. For **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

- **Full sync** – Sync all content regardless of the previous sync status.
- **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

14. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
15. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
16. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

17. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Jira using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- Jira configuration properties
- Jira JSON schema

Jira configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has the following sub-property: `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-property: `jiraAccountUrl` .	Yes
`jiraAccountUrl`	Enter the Jira account URL from your Jira	`string`	Yes

Configuration	Description	Type	Required
	account settings. For example, *https://company.atlassian.net/* .		
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties: `project`, `attachment` , `comment`, `issue`, `worklog`.	Yes
• `project` • `attachment` • `comment` • `issue` • `worklog`	A list of objects that map the attributes or field names of your Jira pages and assets to Amazon Q index field names.	`object` These properties have the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName` • `dateFieldFormat`	Yes
`indexFieldName`	The field name of your Jira project, attachment, comment, issue, or worklog.	`string`	Yes

Configuration	Description	Type	Required
`indexFieldType`	The field type of your Jira project, attachment, comment, issue, or worklog.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes
`dataSourceFieldName`	The data source field name of your Jira project, attachment, comment, issue, or worklog.	`string`	Yes
`dateFieldFormat`	The date format of your Jira project, attachment, comment, issue, or worklog.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties: • isCrawlAcl • isRotateSecret • issuetype • status • fieldForUserId • maxFileSizeInMegaBytes • project • issueSubEntityFilter • inclusionPatterns • exclusionPatterns	Yes

Configuration	Description	Type	Required
`isCrawlAcl`	Specify `true` to crawl access control information from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.	`boolean`	No
`isRotateSecret`	Specify `true` if you want to automatically rotate the secret.	`boolean`	No
`issuetype`	Customize the issue types to crawl.	`array` The allowed values are `Bug`, `Story`, `Epic`, `Task`.	No

Configuration	Description	Type	Required
• `status` • `project` • `issueSubEntityFilter`	Customize the status types, projects, and additional elements to crawl.	`array`	No
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string`	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No

Configuration	Description	Type	Required
`inclusionPatterns`	A list of regular expression patterns to include specific content in your Jira data source. Content that matches the patterns are included in the index. Contents that doesn't match the pattern are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array`	No

Configuration	Description	Type	Required
`exclusionPatterns`	A list of regular expression patterns to exclude specific content in your Jira data source. Content that matches the patterns are excluded from the index. Content that doesn't match the patterns are included in the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array`	No
`type`	The type of data source. Specify `JIRA` as your data source type.	`string`	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/principal information on users and groups with access to specific documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.	`boolean`	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required

`secretArn`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Jira.	`string`
		
		The secret must contain a JSON structure with the following keys:
		
		`{ "Jira ID": "Jira user name or email host URL", "Password/Token": "Jira API token" }`
			Yes

`version`	The version of this template that's currently supported.	`string`	No

Jira JSON schema

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- Jira configuration properties
- Jira JSON schema
- Jira JSON schema example

Jira configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has the following sub-property: `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-property: `jiraAccountUrl` .	Yes
`jiraAccountUrl`	Enter the Jira account URL from your Jira account settings. For example, *`https://company.atlassian.net/`* .	`string`	Yes
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties: `project`, `attachment` , `comment`, `issue`, `worklog`.	Yes

Configuration	Description	Type	Required
• project • attachment • comment • issue • worklog	A list of objects that map the attributes or field names of your Jira pages and assets to Amazon Q index field names.	object These properties have the following sub-properties. • indexFieldName • indexFieldType • dataSourceFieldName • dateFieldFormat	Yes
indexFieldName	The field name of your Jira project, attachment, comment, issue, or worklog.	string	Yes
indexFieldType	The field type of your Jira project, attachment, comment, issue, or worklog.	string The allowed values are STRING, STRING_LIST , and DATE.	Yes
dataSourceFieldName	The data source field name of your Jira project, attachment, comment, issue, or worklog.	string	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The date format of your Jira project, attachment, comment, issue, or worklog.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No
`additionalProperties`	Additional configuration options for your content in your data source.	`object` This property has the following sub-properties: • `isCrawlAcl` • `isRotateSecret` • `issuetype` • `status` • `fieldForUserId` • `maxFileSizeInMegaBytes` • `project` • `issueSubEntityFilter` • `inclusionPatterns` • `exclusionPatterns`	Yes

Configuration	Description	Type	Required
`isCrawlAcl`	Specify `true` to crawl access control information from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.	`boolean`	No
`isRotateSecret`	Specify `true` if you want to automatically rotate the secret.	`boolean`	No
`issuetype`	Customize the issue types to crawl.	`array` The allowed values are `Bug`, `Story`, `Epic`, `Task`.	No

Configuration	Description	Type	Required
• `status` • `project` • `issueSubEntityFilter`	Customize the status types, projects, and additional elements to crawl.	`array`	No
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string`	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No

Configuration	Description	Type	Required
`inclusionPatterns`	A list of regular expression patterns to include specific content in your Jira data source. Content that matches the patterns are included in the index. Contents that doesn't match the pattern are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array`	No

Configuration	Description	Type	Required
`exclusionPatterns`	A list of regular expression patterns to exclude specific content in your Jira data source. Content that matches the patterns are excluded from the index. Content that doesn't match the patterns are included in the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array`	No
`type`	The type of data source. Specify `JIRA` as your data source type.	`string`	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/principal information on users and groups with access to specific documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.	`boolean`	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required

`secretArn`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Jira.	`string`
		
		The secret must contain a JSON structure with the following keys:
		
		`{ "Jira ID": "Jira user name or email host URL", "Password/Token": "Jira API token" }`
			Yes

`version`	The version of this template that's currently supported.	`string`	No

Jira JSON schema

The following is the Jira JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "pattern": "JIRA"
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
```

```
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "jiraAccountUrl": {
              "type": "string",
              "pattern": "https://.*"
            }
          },
          "required": ["jiraAccountUrl"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "attachment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
```

```
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "comment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
```

```
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "issue": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
```

```
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "project": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "worklog": {
      "type": "object",
      "properties": {
```

```
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        }
      }
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "isCrawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
```

```
            "enum": ["true", "false"]
          }
        ]
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "fieldForUserId": {
        "type": "string"
      },
      "issuetype": {
        "type": "array",
        "items": {
          "type": "string",
          "enum": ["Bug", "Story", "Epic", "Task"]
        }
      },
      "status": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "project": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "issueSubEntityFilter": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionPatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionPatterns": {
        "type": "array",
        "items": {
```

```
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "type",
    "syncMode",
    "secretArn",
    "enableIdentityCrawler",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

Jira JSON schema example

The following is the Jira JSON schema example:

```
{
  "type": "JIRA",
  "syncMode": "FULL_CRAWL",
  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-jira-secret",
  "enableIdentityCrawler": "true",
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "jiraAccountUrl": "https://mycompany.atlassian.net"
    }
  },
  "repositoryConfigurations": {
    "attachment": {
      "fieldMappings": [
        {
          "indexFieldName": "attachment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "comment": {
      "fieldMappings": [
        {
          "indexFieldName": "comment_body",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "body",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "issue": {
      "fieldMappings": [
        {
          "indexFieldName": "issue_key",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "key",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
```

```
    },
    "project": {
      "fieldMappings": [
        {
          "indexFieldName": "project_name",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "name",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "worklog": {
      "fieldMappings": [
        {
          "indexFieldName": "worklog_time_spent",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "timeSpent",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    }
  },
  "additionalProperties": {
    "isCrawlAcl": "true",
    "maxFileSizeInMegaBytes": "50",
    "fieldForUserId": "user_id",
    "issuetype": ["Bug", "Story"],
    "status": ["Open", "In Progress"],
    "project": ["Project1", "Project2"],
    "issueSubEntityFilter": ["SubEntity1"],
    "inclusionPatterns": ["*"],
    "exclusionPatterns": ["*.tmp"],
    "enableDeletionProtection": "false",
    "deletionProtectionThreshold": "15"
  }
}
```

Connecting Amazon Q Business to Jira using AWS CloudFormation

You use the AWS::QBusiness::DataSource resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- Jira configuration properties
- Jira JSON schema for using the configuration property with AWS CloudFormation
- Jira YAML schema for using the configuration property with AWS CloudFormation

Jira configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has the following sub-property: `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-property: `jiraAccountUrl` .	Yes
`jiraAccountUrl`	Enter the Jira account URL from your Jira account settings. For example, *`https://`*	`string`	Yes

Configuration	Description	Type	Required
	company.atlassian.net/ .		
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties: `project`, `attachment` , `comment`, `issue`, `worklog`.	Yes
• `project` • `attachment` • `comment` • `issue` • `worklog`	A list of objects that map the attributes or field names of your Jira pages and assets to Amazon Q index field names.	`object` These properties have the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName` • `dateFieldFormat`	Yes
`indexFieldName`	The field name of your Jira project, attachment, comment, issue, or worklog.	`string`	Yes

Configuration	Description	Type	Required
`indexFieldType`	The field type of your Jira project, attachment, comment, issue, or worklog.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes
`dataSourceFieldName`	The data source field name of your Jira project, attachment, comment, issue, or worklog.	`string`	Yes
`dateFieldFormat`	The date format of your Jira project, attachment, comment, issue, or worklog.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties: • isCrawlAcl • isRotateSecret • issuetype • status • fieldForUserId • maxFileSizeInMegaBytes • project • issueSubEntityFilter • inclusionPatterns • exclusionPatterns	Yes

Configuration	Description	Type	Required
`isCrawlAcl`	Specify `true` to crawl access control information from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.	`boolean`	No
`isRotateSecret`	Specify `true` if you want to automatically rotate the secret.	`boolean`	No
`issuetype`	Customize the issue types to crawl.	`array` The allowed values are `Bug`, `Story`, `Epic`, `Task`.	No

Configuration	Description	Type	Required
• `status` • `project` • `issueSubEntityFilter`	Customize the status types, projects, and additional elements to crawl.	`array`	No
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string`	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No

Configuration	Description	Type	Required
`inclusionPatterns`	A list of regular expression patterns to include specific content in your Jira data source. Content that matches the patterns are included in the index. Contents that doesn't match the pattern are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array`	No

Configuration	Description	Type	Required
`exclusionPatterns`	A list of regular expression patterns to exclude specific content in your Jira data source. Content that matches the patterns are excluded from the index. Content that doesn't match the patterns are included in the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array`	No
`type`	The type of data source. Specify `JIRA` as your data source type.	`string`	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/principal information on users and groups with access to specific documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.	`boolean`	Yes

Configuration	Description	Type	Required
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	`string` You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required

`secretArn`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Jira.	`string`
		
		The secret must contain a JSON structure with the following keys:
		
		`{ "Jira ID": "Jira user name or email host URL", "Password/Token": "Jira API token" }`
			Yes

`version`	The version of this template that's currently supported.	`string`	No

Jira JSON schema for using the configuration property with AWS CloudFormation

The following is the Jira JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- Jira JSON schema for using the configuration property with AWS CloudFormation
- Jira JSON schema example for using the configuration property with AWS CloudFormation

Jira JSON schema for using the configuration property with AWS CloudFormation

The following is the Jira JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
  "properties": {
```

```
    "type": {
      "type": "string",
      "pattern": "JIRA"
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "jiraAccountUrl": {
              "type": "string",
              "pattern": "https://.*"
            }
          },
          "required": ["jiraAccountUrl"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "attachment": {
```

```
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "comment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "issue": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
```

```
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "project": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
```

```
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "worklog": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
```

```
    "additionalProperties": {
      "type": "object",
      "properties": {
        "isCrawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        },
        "fieldForUserId": {
          "type": "string"
        },
        "issuetype": {
          "type": "array",
          "items": {
            "type": "string",
            "enum": ["Bug", "Story", "Epic", "Task"]
          }
        },
        "status": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "project": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "issueSubEntityFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
```

```
        },
        "inclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "type",
    "syncMode",
```

```
    "secretArn",
    "enableIdentityCrawler",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

Jira JSON schema example for using the configuration property with AWS CloudFormation

The following is the Jira JSON schema example for the configuration property for CloudFormation

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation JIRA Data Source Template",
  "Resources": {
    "DataSourceJira": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MyJiraDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "JIRA",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-jira-
secret",
          "enableIdentityCrawler": "true",
          "connectionConfiguration": {
            "repositoryEndpointMetadata": {
              "jiraAccountUrl": "https://mycompany.atlassian.net"
            }
          },
          "repositoryConfigurations": {
            "attachment": {
              "fieldMappings": [
                {
                  "indexFieldName": "attachment_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
```

```
      },
      "comment": {
        "fieldMappings": [
          {
            "indexFieldName": "comment_body",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "body",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "issue": {
        "fieldMappings": [
          {
            "indexFieldName": "issue_key",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "key",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "project": {
        "fieldMappings": [
          {
            "indexFieldName": "project_name",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "name",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "worklog": {
        "fieldMappings": [
          {
            "indexFieldName": "worklog_time_spent",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "timeSpent",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      }
    },
    "additionalProperties": {
      "isCrawlAcl": "true",
```

```
            "maxFileSizeInMegaBytes": "50",
            "fieldForUserId": "user_id",
            "issuetype": ["Bug", "Story"],
            "status": ["Open", "In Progress"],
            "project": ["Project1", "Project2"],
            "issueSubEntityFilter": ["SubEntity1"],
            "inclusionPatterns": ["*"],
            "exclusionPatterns": ["*.tmp"],
            "enableDeletionProtection": "false",
            "deletionProtectionThreshold": "15"
          }
        }
      }
    }
  }
}
```

Jira YAML schema for using the configuration property with AWS CloudFormation

The following is the Jira YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- Jira YAML schema for using the configuration property with AWS CloudFormation
- Jira YAML schema example for using the configuration property with AWS CloudFormation

Jira YAML schema for using the configuration property with AWS CloudFormation

The following is the Jira YAML schema for the configuration property for CloudFormation.

```
type: object
properties:
  type:
    type: string
    pattern: JIRA
  syncMode:
    type: string
    enum:
      - FULL_CRAWL
      - FORCED_FULL_CRAWL
      - CHANGE_LOG
  secretArn:
```

```
    type: string
    minLength: 20
    maxLength: 2048
  enableIdentityCrawler:
    anyOf:
      - type: boolean
      - type: string
        enum:
          - true
          - false
  connectionConfiguration:
    type: object
    properties:
      repositoryEndpointMetadata:
        type: object
        properties:
          jiraAccountUrl:
            type: string
            pattern: https://.*
        required:
          - jiraAccountUrl
    required:
      - repositoryEndpointMetadata
  repositoryConfigurations:
    type: object
    properties:
      attachment:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
```

```
            dateFieldFormat:
              type: string
              pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
          required:
            - indexFieldName
            - indexFieldType
            - dataSourceFieldName
      required:
        - fieldMappings
    comment:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    issue:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
```

```
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
        required:
          - fieldMappings
      project:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
```

```
        required:
          - fieldMappings
      worklog:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
  additionalProperties:
    type: object
    properties:
      isCrawlAcl:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      maxFileSizeInMegaBytes:
        type: string
      fieldForUserId:
        type: string
      issuetype:
```

```
        type: array
        items:
          type: string
          enum:
            - Bug
            - Story
            - Epic
            - Task
      status:
        type: array
        items:
          type: string
      project:
        type: array
        items:
          type: string
      issueSubEntityFilter:
        type: array
        items:
          type: string
      inclusionPatterns:
        type: array
        items:
          type: string
      exclusionPatterns:
        type: array
        items:
          type: string
      enableDeletionProtection:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
        default: false
      deletionProtectionThreshold:
        type: string
        default: "15"
  version:
    type: string
    anyOf:
      - pattern: 1.0.0
required:
```

```
  - type
  - syncMode
  - secretArn
  - enableIdentityCrawler
  - connectionConfiguration
  - repositoryConfigurations
  - additionalProperties
```

Jira YAML schema example for using the configuration property with AWS CloudFormation

The following is the Jira YAML example for the Configuration property for CloudFormation:

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation JIRA Data Source Template",
  "Resources": {
    "DataSourceJira": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MyJiraDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "JIRA",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-jira-
secret",
          "enableIdentityCrawler": "true",
          "connectionConfiguration": {
            "repositoryEndpointMetadata": {
              "jiraAccountUrl": "https://mycompany.atlassian.net"
            }
          },
          "repositoryConfigurations": {
            "attachment": {
              "fieldMappings": [
                {
                  "indexFieldName": "attachment_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
```

```
      },
      "comment": {
        "fieldMappings": [
          {
            "indexFieldName": "comment_body",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "body",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "issue": {
        "fieldMappings": [
          {
            "indexFieldName": "issue_key",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "key",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "project": {
        "fieldMappings": [
          {
            "indexFieldName": "project_name",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "name",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "worklog": {
        "fieldMappings": [
          {
            "indexFieldName": "worklog_time_spent",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "timeSpent",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      }
    },
    "additionalProperties": {
      "isCrawlAcl": "true",
```

```
            "maxFileSizeInMegaBytes": "50",
            "fieldForUserId": "user_id",
            "issuetype": ["Bug", "Story"],
            "status": ["Open", "In Progress"],
            "project": ["Project1", "Project2"],
            "issueSubEntityFilter": ["SubEntity1"],
            "inclusionPatterns": ["*"],
            "exclusionPatterns": ["*.tmp"],
            "enableDeletionProtection": "false",
            "deletionProtectionThreshold": "15"
          }
        }
      }
    }
  }
}
```

How Amazon Q Business connector crawls Jira ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

Jira organizes work into Projects, which serve as containers for Issues—the core tasks, bugs, or stories that teams track. Each issue belongs to a project and can have Comments, Attachments, and Worklogs to facilitate collaboration, provide context, and track time spent. Projects can be Team-Managed (private, limited, or open) or Company-Managed, offering flexibility in workflows and permissions. When you connect an Jira data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your Jira instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

Projects

Jira organizes work into Projects, which serve as containers for Issues—the core tasks, bugs, or stories that teams track. Each issue belongs to a project and can have Comments, Attachments, and Worklogs to facilitate collaboration, provide context, and track time spent. Projects can be Team-Managed (private, limited, or open) or Company-Managed, offering flexibility in workflows and permissions. When you connect an Jira data source to Amazon Q Business, Amazon Q

Business crawls ACL information attached to a document (user and group information) from your Jira instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

Identity crawling

The Jira connector extracts project-level permissions based on the project key. It identifies direct users and group members, capturing their account IDs and emails. Federated groups, synchronized from external identity providers, appear as local groups in Jira but are managed externally. The connector respects Jira's permission structure, ensuring that permissions remain intact even when users are removed and later reinstated. Suspended users are included in API responses but marked as inactive, preventing unauthorized access.

> **Note**
>
> For all types of projects, you must have at least 'Browse Projects' permissions (direct or indirect), and Email visibility must be set to "Anyone" for AWS to validate permissions correctly. The "Anyone" email visibility setting is required for proper integration with AWS and other third-party tools due to Jira's API limitations.

Permissions inheritance

Global Permissions determine who can access the Jira instance and perform high-level actions. Project Permissions, governed by permission schemes, define user access within projects, such as viewing, editing, or assigning issues. In Company-Managed projects, permissions flow from the Jira instance down to projects and further to issues, attachments, comments, and worklogs. Issue Security Schemes further restrict access to specific issues within a project. In Team-Managed projects, access is defined by project roles and project visibility settings: **Open** (accessible to all), **Limited** (viewable by all but editable only by members), and **Private** (restricted to project members). While permissions in Company-Managed projects follow a structured hierarchy, Team-Managed projects rely on role-based access. Inheritance applies at the project level, meaning that issues, comments, attachments, and worklogs inherit permissions from their parent project. However, Issue Security Levels can override project permissions by restricting visibility at an issue level.

ACL mapping

Before enabling ACL-based document access for Jira within Amazon Q Business, it is important to understand how permissions and groups are mapped between Jira and Amazon Q, especially given the structural differences between Team-Managed and Company-Managed projects.

Team-Managed Projects: For Team-Managed projects in Jira Software Cloud, ACL mapping is straightforward. The permissions for such projects are configured on the **Project Settings > Access** tab, where you will find a list of users and groups along with their associated project roles. For these projects, a single group is created in Amazon Q Business using the format `projectKey:[ProjectKey]` (for example, `projectKey:TestProject`). This group is attached to all documents under the project, including the project-level document, issues, comments, worklogs, and attachments. All users listed in the **Access** tab will have visibility into all project documents, regardless of their roles.

Company-Managed Projects: Company-Managed projects offer more granular access control and therefore require a more complex mapping strategy. To determine document visibility, it is necessary to review two areas within the Jira project:

- **Project Settings > People**, which lists users and groups along with their project roles. Inclusion in this list does not guarantee document access even for Administrator roles.
- **Project Settings > Permissions** The **Browse Projects** permission governs who can view the project and its issues. This setting can include a variety of grant types, such as specific groups, project roles, individual users, or dynamic conditions like issue assignees. Ensure users have all necessary permissions listed in Prerequisites.

Jira also supports issue-level security, which can override the broader **Browse Projects** settings by enforcing granular access rules on a per-issue basis. You need to consider this label during ACL mapping.

Following is an example of how group mappings in Amazon Q Business for Company-Managed projects are established:

- **Project**: A group named `TestProject` is created, comprising all users who have been granted **Browse Projects** permission, regardless of grant type.
- **Issue-Level Document**: In the example issue `Test1`, group assignments depend on permissions:
- • If a user gains access through project-level permissions, the group `ProjectBasedBrowseKey:Test` is used.

  - If access is granted through dynamic conditions such as the user being the assignee, the group `IssueBasedBrowseKey:Test1` is used.
  - If both types of access mechanisms exist, users may belong to both groups.
- **Issue with Issue-Level Security Enabled**: Access requires both project/issue-based browse permissions and issue-specific security clearance. The condition becomes: `(ProjectBasedBrowseKey:Test OR IssueBasedBrowseKey:Test1) AND IssueLevelKey:Test1`.
- **Comments, Attachments, and Worklog**s: These documents inherit the same access control as the associated issue. Therefore, the same issue-level logic applies..

Change management

Change Log Mode in Amazon Q Business enables incremental updates by capturing modifications made to content in Jira. Instead of re-indexing all documents, it indexes only newly added, updated, or deleted items since the last crawl. Any changes to user or group access permissions are also recorded, ensuring accurate and up-to-date indexing.

Failure handling

The Jira connector follows a fail-close approach, skipping documents from ingestion in case of API failures or permission-related issues. If a document has no ACLs attached and ACL enforcement is enabled by the admin, it will be ingested and made publicly accessible to configured users.

More information

For more information about ACLs, see:

- Authorization
- Identity crawler
- Understanding User Store

Jira data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Jira connector supports the following entities and the associated reserved and custom attributes.

Supported entities and field mappings

- Projects
- Issues
- Comments
- Attachments
- Worklogs

Projects

Jira field name	Index field name	Description	Data type
title	j_title	Custom	String

Jira field name	Index field name	Description	Data type
project_key	j_project_key	Custom	String
lead	j_lead	Custom	String list
url	_source_uri	Default	String

Issues

Jira field name	Index field name	Description	Data type
title	j_title	Custom	String
issue_key	j_issue_key	Custom	String
status	j_status	Custom	String
project_name	j_project_name	Custom	String
projectKey	j_project_key	Custom	String
authors	_authors	Default	String list
assignee	j_assignee	Custom	String
created_at	_created_at	Default	Date
updated_at	_last_updated_at	Default	Date
url	_source_uri	Default	String
issue_type	j_issue_type	Custom	String
priority	j_priority	Custom	String
resolution	j_resolution	Custom	String
affects_version	j_affects_version	Custom	String

Jira field name	Index field name	Description	Data type
fix_version	j_fix_version	Custom	String
labels	j_labels	Custom	String
environment	j_environment	Custom	String
reporter	j_reporter	Custom	String
votes	j_votes	Custom	String
watchers	j_watchers	Custom	String
due	j_due	Custom	String
resolved	j_resolved	Custom	String

Comments

Jira field name	Index field name	Description	Data type
authors	_authors	Default	String list
title	j_title	Custom	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
project_name	j_project_name	Custom	String
project_key	j_project_key	Custom	String
issue_key	j_issue_key	Custom	String
url	_source_uri	Default	String

Attachments

Jira field name	Index field name	Description	Data type
title	j_title	Custom	String
authors	_authors	Default	String list
size	j_size	Custom	String
createdAt	_created_at	Default	Date
url	_source_uri	Default	String
project_name	j_project_name	Custom	String
project_key	j_project_key	Custom	String
issue_key	j_issue_key	Custom	String

Worklogs

Jira field name	Index field name	Description	Data type
title	j_title	Custom	String
authors	_authors	Default	String list
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
url	_source_uri	Default	String
project_name	j_project_name	Custom	String
project_key	j_project_key	Custom	String
issue_key	j_issue_key	Custom	String

IAM role for Amazon Q Business Jira connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
```

```
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
```

```
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
```

```
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the Amazon Q Business Jira connector

The following table provides information about error codes you may see for the Jira connector and suggested resolutions.

Error code	Error message
JIRA-5100	There was a problem while retrievin g access token. Access token should not be null or empty.
JIRA-5101	There was an error parsing the field value. The size has exceeded the maximum allowable limit.
JIRA-5102	Jira inclusion pattern list is too large.
JIRA-5103	Some of the inclusion objects exceed the character limit.
JIRA-5104	Jira exclusion pattern size list is too large.
JIRA-5105	Some of the exclusion objects exceed the character limit.

Error code	Error message
JIRA-5106	There was a problem while retrievin g refresh token. Refresh token should not be null or empty.
JIRA-5107	There was a problem while retrievin g Jira Credential. Jira Credential should not be null or empty.
JIRA-5108	There was a problem while retrievin g Jira Id. Jira Id should not be null or empty.
JIRA-5109	There was a problem while retrievin g Auth Type. Auth Type should not be null or empty.
JIRA-5110	There was a problem while retrievin g Jira Account Url. Jira Account Url should not be null or empty.
JIRA-5111	JIRA Issue Sub Entity Filter list size is too large.
JIRA-5112	Some of the Jira Issue Sub Entity Filter objects exceed the character limit.
JIRA-5113	Jira Issue Status Filter list size is too large.
JIRA-5114	Some of the Jira Issue Status Filter objects exceeded the character limit.
JIRA-5115	Jira Issue Type Filter list size is too large.

Error code	Error message
JIRA-5116	Some of the Jira Issue Type Filter objects exceed the character limit.
JIRA-5117	Jira Project Key Filter list size is too large.
JIRA-5118	Some of the JIRA Project Key Filter objects exceed the character limit.
JIRA-5119	Project specific field mappings are not configured for connector.
JIRA-5120	Issue specific field mappings are not configured for connector.
JIRA-5121	Comment specific field mappings are not configured for connector.
JIRA-5122	Attachment specific field mappings are not configured for connector.
JIRA-5123	Worklog specific field mappings are not configured for connector.
JIRA-5124	There was a problem while retrievin g crawl type. Crawl Type should not be null or empty.

Connecting Microsoft Exchange to Amazon Q Business

You can connect your Microsoft Exchange enterprise messaging system to Amazon Q Business to unlock valuable organizational knowledge. This connection allows your users to search emails, calendar events, and shared content directly through the Amazon Q web experience.

You can connect your Microsoft Exchange instance to Amazon Q Business using the AWS Management Console or the CreateDataSource API. This enables faster information discovery and improved decision-making across your organization.

Topics

- Microsoft Exchange connector versions
- Known limitations for the Microsoft Exchange connector
- Microsoft Exchange connector overview
- Prerequisites for connecting Amazon Q Business to Microsoft Exchange
- Connecting using the Latest Microsoft Exchange Connector (Console)
- Connecting using the Legacy Microsoft Exchange Connector (Console)
- Connecting Amazon Q Business to Microsoft Exchange using APIs
- Connecting Amazon Q Business to Microsoft Exchange (New connector) using APIs
- How Amazon Q Business connector crawls Exchange ACLs
- Microsoft Exchange data source connector field mappings
- IAM role for Microsoft Exchange connector
- Understand error codes in the Microsoft Exchange connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Microsoft Exchange connector versions

You can choose between two Microsoft Exchange connector versions:

Latest Microsoft Exchange connector (Recommended)

> **Note**
>
> The latest connector provides improved accuracy. We recommend using the latest connector for new implementations. The legacy connector remains available if you need specific features not yet supported in the latest connector.

The latest Microsoft Exchange connector offers a simplified configuration experience:

- Enhanced accuracy and performance
- Simplified filtering with Date Range options only
- Automatic crawling of ACL and identity information

Legacy Microsoft Exchange connector

The legacy Microsoft Exchange connector provides full-featured configuration with advanced options:

- Complete entity type selection including Calendar, OneNotes, and Contacts
- Advanced filtering options and regex pattern matching
- Custom field mappings for metadata extraction
- Configurable sync modes and VPC settings
- Domain-based email filtering and inclusion rules
- Manual ACL and identity crawling configuration

Known limitations for the Microsoft Exchange connector

> **Note**
>
> **Legacy version notice:** We recommend using the latest connector for improved performance and retrieval quality. The following limitations apply only to the legacy connector version.

The original Microsoft Exchange connector has these known limitations:

- When you enable Access Control Lists (ACLs), the "Sync only new or modified content" option is not available due to Microsoft Exchange API limitations. Use "Full sync" or "New, modified, or deleted content sync" modes instead, or disable ACLs to use this sync mode.

Microsoft Exchange connector overview

The following table shows the Amazon Q Business Microsoft Exchange connector features and capabilities.

Category	Feature	Latest Connector	Legacy Connector
Security	**Authentication type**	OAuth 2.0 with Client Credentials Flow	OAuth 2.0 with Client Credentials Flow
	Authentication credentials	• Microsoft Exchange Client ID • Microsoft Exchange Client secret	• Microsoft Exchange Client ID • Microsoft Exchange Client secret
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.	Yes. For more information, see ACL crawling.
	Identity crawling	Yes	Yes
	VPC	No	Yes
	Customer Managed Key (CMK) support	No	Yes
Crawl features	**Custom metadata**	No	No
	Entities	Mail only (automatic)	Yes. The following entities are supported: • Mail • Calendar • Attachment

Category	Feature	Latest Connector	Legacy Connector
			• OneNotes • Contacts See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes (Automatic)	Yes. Supports both default and custom field mappings. For more information, see Field mappings.

Category	Feature	Latest Connector	Legacy Connector
	Filters	Date range only	Yes. The following filters are supported: • Include/exclue Calendars • Include/exclude OneNotes • Include/exclude Contacts • Include/exclude using file user email ID • Include/exclude using date • Include/exclude using email to, from, subjects, domains • Include/exclude by file name regex patterns • Include/exclude by file type regex patterns
	Sync mode	Full sync only	Supports full and incremental sync
File types	File types	No	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to Microsoft Exchange

In Microsoft Exchange, make sure you have:

- Created a Microsoft Exchange account in Office 365.
- Copied your Microsoft 365 tenant ID. You can find your tenant ID in the **Properties** of your Azure Active Directory Portal or in the Microsoft Entra Admin portal. For more information, see Find your Microsoft 365 tenant ID on the Microsoft website.
- Configured an OAuth 2.0 credential token containing a client ID and client secret.
- Added the following permissions for the connector application:

Microsoft Graph	Office 365 Exchange Online
• Mail.Read (Application) • Mail.ReadBasic (Application) • Mail.ReadBasic.All (Application) • Calendars.Read (Application) • User.Read.All Application) • Contacts.Read (Application) • Notes.Read.All (Application) • Directory.Read.All (Application) • EWS.AccessAsUser.All (Delegated)	full_access_as_app (Application)

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Microsoft Exchange authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting using the Latest Microsoft Exchange Connector (Console)

The latest Microsoft Exchange connector provides a simplified configuration experience with essential features. The following procedure shows how to connect Amazon Q Business to Microsoft Exchange using the latest connector.

Connecting Amazon Q to Microsoft Exchange using the latest connector

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Microsoft Exchange (latest)** data source to your Amazon Q application.
5. Then, on the **Microsoft Exchange** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, enter the following information:

- **Tenant ID** – Enter your tenant ID. Your Microsoft tenant ID is a globally unique identifier required to configure each connector instance. You can find your tenant ID in the properties section of your Microsoft account dashboard.

8. For **Authentication**, choose between **New** and **Existing**.

   - If you choose **Existing**, choose an existing secret for **Select secret**.

     If you choose **New**, enter the following information in the **New AWS Secrets Manager secret** section:

     i. **Secret name** – Enter a name for your secret.

     ii. For **Client ID** and **Client secret**, enter the authentication credential values that you generated from your Exchange account.

9. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

   > **Note**
   >
   > Creating a new service IAM role is recommended.

   For more information, see IAM role.

10. For **Additional configuration – *optional***, configure the following options:

    - **Date Range** – Enter the date range for crawling your email content. The end date is optional.

    > **Note**
    >
    > **Simplified configuration:** The latest connector automatically crawls email content only with ACL enabled by default. Entity type selection and attachment filtering are not available to keep configuration simple and reliable.

11. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be

skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

1. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
2. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
3. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting using the Legacy Microsoft Exchange Connector (Console)

The legacy Microsoft Exchange connector provides comprehensive configuration options including entity type selection, field mappings, and VPC settings. The following procedure shows how to connect Amazon Q Business to Microsoft Exchange using the legacy connector.

Connecting Amazon Q to Microsoft Exchange using the legacy connector

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Microsoft Exchange** data source to your Amazon Q application.

5. Then, on the **Microsoft Exchange** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, enter the following information:

   - **Tenant ID** – Enter your tenant ID. Your Microsoft tenant ID is a globally unique identifier required to configure each connector instance. You can find your tenant ID in the properties section of your Microsoft account dashboard.
8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
9. **Authentication** – Choose between **New** and **Existing**.

   - If you choose **Existing**, select an existing secret for **Select secret**.

     If you choose **New**, enter the following information in the **New AWS Secrets Manager secret** section:

     i. **Secret name** – A name for your secret.

     ii. For **Client ID**, **Client secret** – Enter the authentication credential values that you generated from your Exchange account.
10. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

11. In **Sync scope**, choose from the following options:
    - **UserIDs** – Choose to filter content by specific user email IDs.
    - **User email ID** – Upload a file with user email IDs to filter content. Format email IDs on separate lines in the file.
    - **Include patterns** – Specify patterns to include specific content.
    - **Exclude patterns** – Specify patterns to exclude specific content.
12. For **Maximum file size**, specify the file size limit in MBs that Amazon Q will crawl. Amazon Q crawls only files within the size limit you define. The default file size is 50MB. The maximum file size must be greater than 0MB and less than or equal to 50MB.
13. For **Additional configuration – *optional***, configure the following options:
    - **Entity types** – Choose whether to crawl the following entities: **Calendar**, **OneNotes**, and **Contacts**.
    - **Calendar crawling** – Enter the date range for which the connector will crawl your calendar content.
    - **Include email** – Enter the email from domains, email to domains, and subjects you wish to include or exclude in your application.
    - **Shared folders access** – Enable ACL crawling for shared folders.
    - **Regex for domains** – Add patterns to include and exclude certain email domains from your application.
    - **Regex patterns** – Add regular expression patterns to include or exclude certain files. You can add up to 100 patterns.
14. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

    To extract audio transcriptions and video content, enable processing for the following file types:

15. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

1. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
2. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
3. **Field mappings** – A list of data source document attributes to map to your index fields.

   > **Note**
   >
   > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

   a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

   b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

      > **Note**
      >
      > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

   For more information, see Field mappings.
4. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

For more information, see VPC.

5. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Microsoft Exchange using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Microsoft Exchange JSON schema

The following shows the Microsoft Exchange JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            }
          },
          "required": ["tenantId"]
        }
      }
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "email": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
```

```
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": [
            "fieldMappings"
          ]
        },
        "attachment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE","LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
```

```
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "calendar": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
```

```
          },
          "required": [
            "fieldMappings"
          ]
        },
        "contacts": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": [
            "fieldMappings"
          ]
        },
        "notes": {
          "type": "object",
```

```
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": [
            "fieldMappings"
          ]
        }
      },
      "required": ["email"
      ]
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "inclusionPatterns": {
          "type": "array",
```

```
          "items": {
            "type": "string"
          }
        },
        "exclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionUsersList": {
          "type": "array",
          "items": {
            "type": "string",
            "format": "email"
          }
        },
        "exclusionUsersList": {
          "type": "array",
          "items": {
            "type": "string",
            "format": "email"
          }
        },
        "s3bucketName": {
          "type": "string"
        },
        "inclusionUsersFileName": {
          "type": "string"
        },
        "exclusionUsersFileName": {
          "type": "string"
        },
        "inclusionDomainUsers": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionDomainUsers": {
          "type": "array",
          "items": {
            "type": "string"
          }
```

```
        },
        "crawlCalendar": {
          "type": "boolean"
        },
        "crawlNotes": {
          "type": "boolean"
        },
        "crawlContacts": {
          "type": "boolean"
        },
        "crawlFolderAcl": {
          "type": "boolean"
        },
        "startCalendarDateTime": {
          "anyOf": [
            {
              "type": "string",
              "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
            },
            {
              "type": "string",
              "pattern": ""
            }
          ]
        },
        "endCalendarDateTime": {
          "anyOf": [
            {
            "type": "string",
            "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
            },
            {
              "type": "string",
              "pattern": ""
            }
          ]
        },
        "subject": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "emailFrom": {
```

```
          "type": "array",
          "items": {
            "type": "string",
            "format": "email"
          }
        },
        "emailTo": {
          "type": "array",
          "items": {
            "type": "string",
            "format": "email"
          }
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        }
      },
      "required": []
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "type" : {
      "type" : "string",
      "pattern": "MSEXCHANGE"
    },
    "secretArn": {
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
```

```
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the endpoint for the data source.
`repositoryEndpointMetadata`	The endpoint information for the data source.
`tenantId`	The Microsoft 365 tenant ID. You can find your tenant ID in the Properties of your Azure Active Directory Portal.
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.
• `email` • `attachment` • `calendar` • `contacts` • `notes`	A list of objects that map the attributes or field names of your Microsoft Exchange data source.
`secretARN`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Exchange data source. This includes your client ID and your client secret.

Configuration	Description
`additionalProperties`	Additional configuration options for content in your data source
`inclusionPatterns` • `inclusionUsersList` • `inclusionUsersFileName` • `inclusionDomainUsers`	A list of regular expression patterns to *include* specific files in your Exchange data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.
`exclusionPatterns` • `exclusionUsersList` • `exclusionUsersFileName` • `exclusionDomainUsers`	A list of regular expression patterns to *exclude* specific files in your Exchange data source. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an exclusion and inclusion pattern, the exclusion pattern takes precedenc e and the file isn't included in the index.
`startCalendarDateTime`	Use to specify the date and time for Calendar content to be crawled by Amazon Q.
`endCalendarDateTime`	Use to specify the date and time for Calendar content to be crawled by Amazon Q.
`subject`	Use to specify email subject lines to be crawled.
`emailFrom`	Use to specify emails to be crawled based on sender.
`emailTo`	Use to specify emails to be crawled based on recipient.

Configuration	Description
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
• `crawlCalendar` • `crawlNotes` • `crawlContacts` • `crawlFolderAcl`	`true` to index this content in your Microsoft Exchange data source. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index

Configuration	Description
`type`	The type of data source. Specify `MSEXCHANGE` as your data source type.
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.
`version`	The version of this template that's currently supported.

Connecting Amazon Q Business to Microsoft Exchange (New connector) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Microsoft Exchange new connector JSON schema

The following shows the Microsoft Exchange new connector JSON schema:

```
{
    "$schema": "http://json-schema.org/draft-07/schema#",
    "type": "object",
    "properties": {
        "type": {
            "type": "string",
            "enum": ["MSEXCHANGEV2"]
        },
        "connectionConfiguration": {
            "type": "object",
            "properties": {
                "secretArn": {
                    "type": "string",
                    "pattern": "^arn:[a-z0-9-\\.]{1,63}:[a-z0-9-\\.]{0,63}:[a-z0-9-\\.]
{0,63}:[a-z0-9-\\.]{0,63}:[^/].{0,1023}$"
                },
                "tenantId": {
                    "type": "string",
                    "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[4][0-9a-f]{3}-[89ab][0-9a-f]
{3}-[0-9a-f]{12}$",
                    "minLength": 36,
                    "maxLength": 36
                }
            },
            "required": ["tenantId", "secretArn"]
        },
        "dataEntityConfiguration": {
            "type": "object",
            "properties": {
            }
        },
        "filterConfiguration": {
            "type": "object",
            "properties": {
                "startDateFilter": {
                    "type": "string",
                    "format": "date-time"
                },
                "endDateFilter": {
                    "type": "string",
```

```
                    "format": "date-time"
                }
            }
        },
        "deletionProtectionConfiguration": {
            "type": "object",
            "properties": {
                "enableDeletionProtection": {
                    "type": "boolean"
                },
                "deletionProtectionThreshold": {
                    "type": "string",
                    "pattern": "^(100|[1-9][0-9]?)$"
                }
            },
            "required": ["enableDeletionProtection", "deletionProtectionThreshold"]
        }
    },
    "required": [
        "type",
        "connectionConfiguration",
        "dataEntityConfiguration"
    ]
}
```

The following table provides information about important JSON keys to configure for the new Microsoft Exchange connector.

Configuration	Description
`type`	The type of data source. Specify `MSEXCHANGEV2` for the new Microsoft Exchange connector.
`connectionConfiguration`	Configuration information for connecting to the Microsoft Exchange data source.
`secretArn`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your

Configuration	Description
	Exchange data source. This includes your client ID and your client secret.
`tenantId`	The Microsoft 365 tenant ID (UUID v4 format). You can find your tenant ID in the Properties of your Azure Active Directory Portal.
`dataEntityConfiguration`	Configuration for the types of data entities to crawl from Microsoft Exchange.
`filterConfiguration`	Optional configuration for filtering content during the crawl process.
`startDateFilter`	Specify the start date for filtering emails. Only emails created on or after this date will be crawled. Format: ISO 8601 date-time (e.g., `2025-06-01T00:00:00Z`).
`endDateFilter`	Specify the end date for filtering emails. Only emails created on or before this date will be crawled. Format: ISO 8601 date-time (e.g., `2025-07-01T00:00:00Z`).
`deletionProtectionConfiguration`	Optional configuration to protect against accidental deletion of large amounts of content.
`enableDeletionProtection`	A Boolean value to enable deletion protectio n. When enabled, the connector will not delete more than the specified threshold of documents in a single sync.
`deletionProtectionThreshold`	The maximum percentage of documents that can be deleted in a single sync when deletion protection is enabled. Must be a string representing a number from 1-100 (e.g., "10" for 10%).

Sample configuration for the new Microsoft Exchange connector

The following is a sample configuration for the new Microsoft Exchange connector:

```
{
    "displayName": "mail-0910-sample",
    "configuration": {
        "connectionConfiguration": {
            "secretArn": "arn:aws:secretsmanager:<region>:<account>:secret:<secret>",
            "tenantId": "<tenant_id>"
        },
        "dataEntityConfiguration": {
        },
        "filterConfiguration": {
            "startDateFilter": "2025-06-01T00:00:00Z",
            "endDateFilter": "2025-07-01T00:00:00Z"
        },
        "deletionProtectionConfiguration": {
            "enableDeletionProtection": true,
            "deletionProtectionThreshold": "10"
        },
        "type": "MSEXCHANGEV2",
        "version": "1.0.0"
    },
    "description": "Sample Config",
    "syncSchedule": "",
    "roleArn": "arn:aws:iam::<account>:role/service-role/<role_name>",
    "mediaExtractionConfiguration": {}
}
```

Note

ACL crawling is available for both new and original Microsoft Exchange connector versions.

How Amazon Q Business connector crawls Exchange ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an Exchange data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your Exchange instance. If you choose to activate ACL crawling, this information can be used to filter chat responses to your end user's document access level.

The Exchange group and user IDs are mapped as follows:

- `_tenant_id` – Your Microsoft tenant ID is a globally unique identifier required to configure each connector instance. You can find your tenant ID in the properties section of your Microsoft account dashboard.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

> **Note**
>
> Field mappings are available for the original Microsoft Exchange connector only. The new connector uses automatic field mapping.

Microsoft Exchange data source connector field mappings

You can improve search results and customize your users' chat experience by mapping document attributes from your Microsoft Exchange data to fields in your Amazon Q index.

Amazon Q offers two types of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have an attribute mapping already available, or if you want to map additional document attributes to index fields, use custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

Important

Filtering using document attributes in chat is only supported through the API.

Note

You can map any Exchange field to the document title or document body Amazon Q reserved/default index fields.

Supported entities and field mappings

- Mails
- Calendar
- Attachments
- OneNotes
- Contacts

Mails

Microsoft Exchange field name	Index field name	Description	Data type
createdDateTime	_created_at	Default	Date

Microsoft Exchange field name	Index field name	Description	Data type
lastModifiedDateTime	_last_updated_at	Default	Date
uri	_source_uri	Default	String
category	_category	Default	String
bccRecipients	xchng_bccRecipient	Custom	String list
ccRecipients	xchng_ccRecipient	Custom	String list
hasAttachment	xchng_hasAttachment	Custom	String
sendDateTime	xchng_sendDateTime	Custom	Date
importance	xchng_importance	Custom	String
from	xchng_from	Custom	String
to	xchng_to	Custom	String list
receivedDateTime	xchng_receivedDateTime	Custom	Date
isRead	xchng_isRead	Custom	String
replyTo	xchng_replyTo	Custom	String
folder	xchng_folder	Custom	String
title	xchng_title	Custom	String
flagStatus	xchng_flagStatus	Custom	String

Calendar

Microsoft Exchange field name	Index field name	Description	Data type
location	xchng_location	Custom	String
organizer	xchng_organizer	Custom	String
subject	xchng_subject	Custom	String
weblink	_source_uri	Default	String
createdDateTime	_created_at	Default	Date
lastModifiedDateTime	_last_updated_at	Default	Date
eventStartTime	xchng_eventStartTime	Default	Date
eventEndTime	xchng_eventEndTime	Default	Date
attendees	xchng_attendees	Custom	String
recurrence	xchng_Recurrence	Custom	String
category	_category	Default	String
isReminderOn	xchng_isReminderOn	Custom	String
sensitivity	xchng_sensitivity	Custom	String
isOnlineMeeting	xchng_isOnlineMeeting	Custom	String
seriesMasterId	xchng_seriesMasterId	Custom	String
isCancelled	xchng_isCancelled	Custom	String

Attachments

Microsoft Exchange field name	Index field name	Description	Data type
title	xchng_title	Custom	String
lastModifiedDateTime	_last_updated_at	Default	Date
category	_category	Default	String
contentType	_file_type	Default	String
size	xchng_size	Custom	String
url	_source_uri	Default	String

OneNotes

Microsoft Exchange field name	Index field name	Description	Data type
isShared	xchng_isShared	Custom	String
link	xchng_links	Custom	String
title	xchng_title	Custom	String
lastUpdatedBy	xchng_lastUpdatedBy	Custom	String
lastModifiedDateTime	_last_updated_at	Default	Date
createdDateTime	_created_at	Default	Date
category	_category	Default	String
createdBy	xchng_createdBy	Custom	String

Microsoft Exchange field name	Index field name	Description	Data type
userRole	xchng_useRole	Custom	String

Contacts

Microsoft Exchange field name	Index field name	Description	Data type
contactName	xchng_contactName	Custom	String
emailAddress	xchng_email	Custom	String
companyName	xchng_company Name	Custom	String
manager	xchng_manager	Custom	String
jobTitle	xchng_jobtitle	Custom	String
location	xchng_officeLocation	Custom	String
mobilePhone	xchng_mobile	Custom	String
birthday	xchng_birthday	Custom	Date
homeAddress	xchng_homeAddress	Custom	String
businessAddress	xchng_businessAddress	Custom	String
department	xchng_department	Custom	String
profession	xchng_profession	Custom	String
createdAt	_created_at	Default	Date
category	_category	Default	String

Microsoft Exchange field name	Index field name	Description	Data type
url	_source_uri	Custom	String

IAM role for Microsoft Exchange connector

> **Note**
>
> This section applies to both new and original Microsoft Exchange connector versions.

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
```

```
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
```

```
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
```

```
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the Microsoft Exchange connector

The following table provides information about error codes you may see for the Microsoft Exchange connector and suggested resolutions.

Error code	Error message	Suggested resolution
MSE-5101	Exception occurred while validating the configura tions.	Error occurred while validating the configurations. Verify the configura tions and try again.
MSE-5102	Invalid clientId pattern.	Error occurred while validating the configurations. Verify the configura tions and try again.

Error code	Error message	Suggested resolution
MSE-5103	ClientSecret Over maximum length.	Error occurred while validating the configurations. Verify the configura tions and try again.
MSE-5104	Enter valid credentials. Client ID should not be null or empty.	Error occurred while validating the configurations. Client ID should not be null.
MSE-5105	Enter valid credentials. Client Secret should not be null or empty.	Error occurred while validating the configurations. Client Secret should not be null.
MSE-5106	Enter valid credentials. Tenant ID should not be null or empty	Error occurred while validating the configurations. Tenant ID should not be null.
MSE-5107	The provided client ID is invalid.Please verify the client ID and try again.	Provide client id is invalid while doing authentication. Connection will be unsuccessful. Provide valid client id.
MSE-5108	The provided client secret is invalid. Verify the client secret and try again.	Provide client secret is invalid while doing authentication. Connection will be unsuccessful. Provide valid client secret.
MSE-5109	The provided tenant ID is invalid. Please verify the tenant ID and try again.	Provide tenant ID is invalid while doing authentication. Connection will be unsuccessful. Provide valid tenant ID.
MSE-5200	Got exception from customer while accessing the list of users.	Error occurred while fetching the list of users from Microsoft Graph API. Check logs for more details.
MSE-5201	Got exception from customer while accessing mails.	Error occurred while fetching mails from Microsoft Graph API. Check logs for more details.

Error code	Error message	Suggested resolution
MSE-5202	Got exception from customer while accessing calendar events.	Error occurred while fetching calendar events from Microsoft Graph API. Check logs for more details.
MSE-5203	Got exception from customer while accessing OneNotes.	Error occurred while fetching one notes from Microsoft Graph API. Check logs for more details.
MSE-5204	Got exception from customer while accessing attachments.	Error occurred while fetching attachments from Microsoft Graph API. Check logs for more details.
MSE-5205	Got exception from customer while accessing contacts.	Error occurred while fetching contacts from Microsoft Graph API. Check logs for more details.
MSE-5206	Error occurred while retrying API requests.	Error occurred while retrying API requests to fetch data from Microsoft Graph API.
MSE-5301	Got exception from customer while running changelog mode.	Error occurred while handling changelog token. Refer logs or contact connector team for more information.

Connecting Microsoft OneDrive to Amazon Q Business

Microsoft OneDrive is a cloud-based storage service that you can use to store, share, and host your content. You can connect Microsoft OneDrive instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

After you integrate Amazon Q with Microsoft OneDrive, users can ask questions about content stored in their OneDrive repositories. For example, users can inquire about project timelines in Excel spreadsheets, key findings from Word documents, presentation highlights from PowerPoint files, or search for specific information across multiple document types. The integration enables users to quickly access and understand information from their OneDrive content, regardless of file location or type, while providing contextual details such as publication dates, modification history,

and document ownership—all contributing to more efficient information discovery and better-informed decision making.

Topics

- Connecting Microsoft OneDrive to Amazon Q Business (New)
- Connecting Microsoft OneDrive to Amazon Q Business (Original)

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Connecting Microsoft OneDrive to Amazon Q Business (New)

> **Note**
>
> **Enhanced Version:** With the new connector, you can refresh your index significantly faster than before, control the sync scope using a date filter, automatically discover and index content for all users within your Microsoft tenant, and enable Q&A capabilities for audio and video files stored in OneDrive.

Limitations

The Microsoft OneDrive new connector has the following known limitations:

- No support for syncing OneNote files
- Custom field mappings are not supported
- VPC configuration is not supported
- Document enrichment is not supported

- OneDrive API throttling limits are determined by your organization's Microsoft 365 license count and are applied at the application level within a tenant (see this Microsoft documentation). These limits affect how many documents can be synced in a day, with further restrictions when Access Control Lists (ACLs) are involved. For example, in organizations with fewer than 1000 licenses, the connector can sync up to 1.2 million documents per day without ACLs. However, when syncing with ACLs, this limit is reduced to approximately 200,000 documents per day since ACLs require 5 additional resource units. If the sync job exceeds these limits, the OneDrive connector automatically pauses and resumes the following day to sync the remaining documents.

Overview

The following table gives an overview of the Amazon Q Business Microsoft OneDrive new connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	OAuth 2.0 with Client Credentials Flow
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes.
Crawl features	**Entities**	Yes. The following entities are supported: • File See What is a document? for more details on what each connector crawls as a document.
	Filters	Yes. The following filters are supported: • Filter by date • Include or exclude using file path
	Sync mode	Incremental sync only (automatic).

Category	Feature	Support
	File types	Supports all file types supported by Amazon Q.

Prerequisites

Before you begin, make sure that you have completed the following prerequisites.

In your Azure Active Directory (AD) application, make sure you have:

- Created an Azure Active Directory (AD) application.
- Used the AD application ID to register a secret key for the application on the AD site. The secret key must contain the client ID and client secret.
- Copied the AD domain of the organization.
- Added the following Application API permissions to your AD application on the Microsoft Graph option:
  - Read files in all site collections (`Files.Read.All`)
  - Read all users' full profiles (`User.Read.All`)
  - Read all groups (`Group.Read.All`)

> **Note**
>
> Choose the Application permissions type instead of Delegated permissions while adding the API permissions.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Microsoft OneDrive authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Using the console

The following procedure outlines how to connect Amazon Q Business to Microsoft OneDrive using the new connector with the AWS Management Console.

Connecting Amazon Q to Microsoft OneDrive new connector

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Microsoft OneDrive** data source to your Amazon Q application.
5. Then, on the **Microsoft OneDrive** data source page, enter the following information:
6. In **Source**, enter the following information:
   - **OneDrive Tenant ID** Enter your OneDrive Tenant ID without the protocol. You can find your OneDrive Tenant ID under Directory ID in the Microsoft Entra ID (formerly Azure AD) admin center.
7. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
8. In **Authentication** – Choose between **New** and **Existing**.
   - If you choose **Existing**, select an existing secret for **Select secret**.

If you choose **New**, enter the following information in the **New AWS Secrets Manager secret** section:

i. **Secret name** – A name for your secret.

ii. For **Client ID** and **Client secret** – Enter the authentication credential values from your OneDrive account and then choose **Save authentication**.

9. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> IAM roles used for applications can't be used for data sources. If you are unsure if an existing role is used for an application, choose **Create a new role** to avoid errors.

10. In **Sync scope**, configure which OneDrive users and content to sync:

a. **Select OneDrive users** – Choose how to specify which users' content to sync:

- **All users** – Select this option to sync content for all users in the organization. This allows comprehensive content discovery across all user accounts.
- **Users from a user name file** – Choose this option to specify users via a file stored in an Amazon S3 bucket. Select the location of the user name file by choosing **Browse**.

> **Note**
>
> If you choose this option, the IAM role for the data source must have read permissions for the Amazon S3 bucket where the file is stored.

- **Specific users** – Choose this option to manually specify individual users. You can add a maximum of 10 users using this option. To add more than 10 users, create a file containing the usernames and choose **Users from a user name file**.

b. **Maximum single file size** – Set the maximum file size for crawling. During this ingestion, there are file size limits depending on the file type. Video files have a limit of up to 10 GB/10,240 MB. Audio files have a 2 GB/2,048 MB limit. PDF/Word/Powerpoint documents have a 500 MB limit. Excel and other supported file formats have a 50 MB limit. There are also limits to the amount of text extracted from these documents. CSV and Excel

have a extracted text limit of 10MB, all other document formats have a limit of 30MB of extracted text.

c. **Additional configuration - *optional*** – All content will be indexed by default. However, you can also limit the scope with these additional options:

   i. **Date filter** – Add a date range to filter content based on the last modified date:

      - **Start date** – Filter content modified after this date (YYYY/MM/DD format)
      - **End date - optional** – Filter content modified before this date (YYYY/MM/DD format)

   ii. **Filter patterns** – Add file path patterns to include or exclude certain folders and files from OneDrive:

      - **Include patterns** – Specify file paths to include in the sync. Enter the path pattern and choose **Add**.
      - **Exclude patterns** – Specify file paths to exclude from the sync. Enter the path pattern and choose **Add**.

        You can identify the path of a folder or file by following these instructions by (within OneDrive), navigating to the file or folder for which you want to apply a filte and clicking on the three-dot menu button next to the file/folder name and selecting "Details." In the following details panel, scroll down to the "Path" details and click on the "Copy" button next to the path. For shared folders and files, first click on “Open location” in the menu adjacent to the file or the folder name, and then follow the above directions.

d. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**. For more information, see Extracting semantic meaning from embedded images and visuals.

   To extract audio transcriptions and video content, enable **Audio Files**. To extract video content, enable **Video files**. For more information, see Extracting semantic meaning from audio and video Content.

e. **Advanced settings**

   Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete

phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

11. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
12. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
13. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Microsoft OneDrive using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Microsoft OneDrive JSON schema

The following is the Microsoft OneDrive JSON schema for OneDrive:

```
{
```

```
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "version": {
      "type": "string",
      "pattern": "2.0.0"
    },
    "type": {
      "type": "string",
      "enum": [
        "ONEDRIVEV3"
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "secretArn": {
          "type": "string",
          "pattern": "^arn:[a-z0-9-\\.]{1,63}:[a-z0-9-\\.]{0,63}:[a-z0-9-\\.]{0,63}:[a-
z0-9-\\.]{0,63}:[^/].{0,1023}$"
        },
        "tenantId": {
          "type": "string",
          "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$",
          "minLength": 36,
          "maxLength": 36
        },
        "authType": {
          "type": "string",
          "enum": [
            "ENTRA_APP_ID",
            "OAUTH2"
          ]
        }
      },
      "required": [
        "secretArn",
        "tenantId",
        "authType"
      ]
    },
    "dataEntityConfiguration": {
      "type": "object",
      "properties": {
```

```
        "crawlPersonalDrives": {
          "type": "boolean"
        }
      }
    },
    "filterConfiguration": {
      "type": "object",
      "properties": {
        "exclusionUserEmailAddresses": {
          "type": "array",
          "maxItems": 100,
          "items": {
            "type": "string",
            "minLength": 1,
            "maxLength": 1024
          }
        },
        "inclusionUserEmailAddresses": {
          "type": "array",
          "maxItems": 100,
          "items": {
            "type": "string",
            "minLength": 1,
            "maxLength": 1024
          }
        },
        "userFilterPath": {
          "type": "string",
          "pattern": "^s3:\\/\\/[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]\\/.*$"
        },
        "exclusionDriveItems": {
          "type": "array",
          "maxItems": 100,
          "items": {
            "type": "string",
            "minLength": 1,
            "maxLength": 1024
          }
        },
        "inclusionDriveItems": {
          "type": "array",
          "maxItems": 100,
          "items": {
            "type": "string",
```

```
            "minLength": 1,
            "maxLength": 1024
          }
        },
        "absoluteDateBefore": {
          "type": "string",
          "pattern": "^\\d{4}-\\d{2}-\\d{2}T\\d{2}:\\d{2}:\\d{2}(?:\\.\\d+)?(?:Z|[+-]\
\d{2}:\\d{2})$"
        },
        "absoluteDateAfter": {
          "type": "string",
          "pattern": "^\\d{4}-\\d{2}-\\d{2}T\\d{2}:\\d{2}:\\d{2}(?:\\.\\d+)?(?:Z|[+-]\
\d{2}:\\d{2})$"
        },
        "maxFileSizeInMegaBytes": {
          "type": "string",
          "pattern": "^\\d+$"
        }
      }
    },
    "deletionProtectionConfiguration": {
      "type": "object",
      "properties": {
        "enableDeletionProtection": {
          "type": "boolean"
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "pattern": "^(100|[1-9][0-9]?)$"
        }
      }
    },
    "crawlIdentities": {
      "type": "boolean"
    },
    "accessControlConfiguration": {
      "type": "object",
      "properties": {
        "crawlAcls": {
          "type": "boolean"
        }
      }
    }
  },
```

```
  "required": [
    "connectionConfiguration",
    "dataEntityConfiguration",
    "type"
  ]
}
```

The following table provides information about important JSON keys to configure for OneDrive (New).

Configuration	Description
`accessControlConfiguration`	Configuration for access control: `crawlAcls` : Boolean flag to enable/disable crawling of access control lists. Specify `true` to crawl access control information from documents. Amazon Q crawls ACL information by default to ensure responses are generated only from documents your end users have access to.
`crawlIdentities`	Boolean flag to enable/disable crawling of identity information. `true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents.
`deletionProtectionConfiguration`	Configuration for deletion protection: `enableDeletionProtection` : Boolean flag to enable/disable deletion protectio n. `deletionProtectionThreshold` : Threshold percentage (1-100) for deletion protection.
`filterConfiguration`	Configuration for filtering content:

Configuration	Description
	• `exclusionUserEmailAddresses` : List of user email addresses to exclude from crawling. • `inclusionUserEmailAddresses` : List of user email addresses to include in crawling. • `userFilterPath` : S3 path for user filter file. • `exclusionDriveItems` : List of drive items to exclude. • `inclusionDriveItems` : List of drive items to include. • `absoluteDateBefore` : Filter for content modified before this date. • `absoluteDateAfter` : Filter for content modified after this date. • `maxFileSizeInMegaBytes` : Maximum single file size limit in MBs that Amazon Q will crawl.
`dataEntityConfiguration`	Configuration for what content to crawl: `crawlPersonalDrives` : Boolean flag to enable/disable crawling of personal drives.

Configuration	Description
`connectionConfiguration`	Configuration information for connectin g to OneDrive: `secretArn` : The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains authentication credentials. The secret must contain a JSON structure with the following keys: `{"clientI D": "OAuth Client ID", "clientSe cret": "client secret"}` `.tenantId`: The tenant ID in UUID format. `authType`: Authentication type, either "ENTRA_APP_ID" or "OAUTH2".
`type`	The type of data source. Specify `ONEDRIVEV 3` as your data source type.
`version`	The version of this template. Currently supported version is "2.0.0".

Connecting Amazon Q Business to Microsoft OneDrive using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- Microsoft OneDrive JSON schema for using the configuration property with AWS CloudFormation
- Microsoft OneDrive YAML schema for using the configuration property with AWS CloudFormation

Microsoft OneDrive JSON schema for using the configuration property with AWS CloudFormation

The following is the Microsoft OneDrive JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- Microsoft OneDrive JSON schema for using the configuration property with AWS CloudFormation
- Microsoft OneDrive JSON schema example for using the configuration property with AWS CloudFormation

Microsoft OneDrive JSON schema for using the configuration property with AWS CloudFormation

The following is the Microsoft OneDrive JSON schema for the configuration property for CloudFormation.

```
{
    "type": "object",
    "properties": {
        "version": {
            "type": "string"
        },
        "type": {
            "type": "string",
            "enum": ["ONEDRIVEV3"]
        },
        "connectionConfiguration": {
            "type": "object",
            "properties": {
                "secretArn": {
                    "type": "string",
                    "minLength": 20,
                    "maxLength": 2048
                },
                "tenantId": {
                    "type": "string",
                    "minLength": 36,
                    "maxLength": 36
                },
```

```
                "authType": {
                    "type": "string",
                    "enum": ["OAUTH2"]
                }
            },
            "required": ["secretArn", "tenantId", "authType"]
        },
        "dataEntityConfiguration": {
            "type": "object",
            "properties": {
                "crawlPersonalDrives": {
                    "anyOf": [{
                            "type": "boolean"
                        },
                        {
                            "type": "string",
                            "enum": ["true", "false"]
                        }
                    ]
                }
            }
        },
        "filterConfiguration": {
            "type": "object",
            "properties": {
                "inclusionUserEmailAddresses": {
                    "type": "array",
                    "maxItems": 100,
                    "items": {
                        "type": "string",
                        "minLength": 1,
                        "maxLength": 1024
                    }
                },
                "userFilterPath": {
                    "type": "string",
                    "minLength": 1,
                    "maxLength": 1024
                },
                "exclusionDriveItems": {
                    "type": "array",
                    "maxItems": 100,
                    "items": {
                        "type": "string",
```

```
                        "minLength": 1,
                        "maxLength": 1024
                    }
                },
                "inclusionDriveItems": {
                    "type": "array",
                    "maxItems": 100,
                    "items": {
                        "type": "string",
                        "minLength": 1,
                        "maxLength": 1024
                    }
                },
                "absoluteDateBefore": {
                    "type": "string",
                    "description": "ISO 8601 date-time format (e.g.,
2024-12-31T23:59:59Z)"
                },
                "absoluteDateAfter": {
                    "type": "string",
                    "description": "ISO 8601 date-time format (e.g.,
2024-12-31T23:59:59Z)"
                },
                "maxFileSizeInMegaBytes": {
                    "type": "string"
                }
            }
        },
        "deletionProtectionConfiguration": {
            "type": "object",
            "properties": {
                "enableDeletionProtection": {
                    "anyOf": [{
                            "type": "boolean"
                        },
                        {
                            "type": "string",
                            "enum": ["true", "false"]
                        }
                    ]
                },
                "deletionProtectionThreshold": {
                    "type": "string",
                    "description": "percentage value of range (0-100)"
```

```
                }
            }
        },
        "crawlIdentities": {
            "anyOf": [{
                    "type": "boolean"
                },
                {
                    "type": "string",
                    "enum": ["true", "false"]
                }
            ]
        },
        "accessControlConfiguration": {
            "type": "object",
            "properties": {
                "crawlAcl": {
                    "anyOf": [{
                            "type": "boolean"
                        },
                        {
                            "type": "string",
                            "enum": ["true", "false"]
                        }
                    ]
                }
            }
        },
        "identityLoggingStatus": {
            "type": "string",
            "enum": ["ENABLED", "DISABLED"]
        },
    },
    "required": ["connectionConfiguration", "dataEntityConfiguration", "type"]
}
```

Microsoft OneDrive JSON schema example for using the configuration property with AWS CloudFormation

The following is the Microsoft OneDrive JSON example for the Configuration property for CloudFormation.

```
{
```

```
    "type": "ONEDRIVEV3",
    "crawlIdentities": false,
    "connectionConfiguration": {
      "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-one-drive-
secret",
      "tenantId": "1234a12c-1234-1234-1abc-1234ab12a12a",
      "authType": "OAUTH2"
    },
    "dataEntityConfiguration": {
      "crawlPersonalDrives": true
    },
    "accessControlConfiguration": {
      "crawlAcl": false
    },
    "filterConfiguration": {
      "inclusionUserEmailAddresses": ["user123@amazon.com"],
      "maxFileSizeInMegaBytes": "50",
      "exclusionDriveItems": ["path/to/folder1","path/to/file1"],
       "inclusionDriveItems": ["path/to/folder2","path/to/file2"],
       "userFilterPath": "s3://bucket/prefix/object.txt",
       "absoluteDateBefore": "2025-08-02T00:00:00Z",
       "absoluteDateAfter": "2025-08-01T00:00:00Z"
    },
    "deletionProtectionConfiguration": {
      "enableDeletionProtection": true,
      "deletionProtectionThreshold": "10"
    },
    "version": "3.0.0",
    "identityLoggingStatus": "DISABLED"
}
```

Microsoft OneDrive YAML schema for using the configuration property with AWS CloudFormation

The following is the Microsoft OneDrive YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- Microsoft OneDrive YAML schema for using the configuration property with AWS CloudFormation
- Microsoft OneDrive YAML schema example for using the configuration property with AWS CloudFormation

Microsoft OneDrive YAML schema for using the configuration property with AWS CloudFormation

The following is the Microsoft OneDrive YAML schema for the configuration property for CloudFormation.

```
configuration:
  type: object
  properties:
    version:
      type: string
    type:
      type: string
      enum:
        - ONEDRIVEV3
    connectionConfiguration:
      type: object
      properties:
        secretArn:
          type: string
          minLength: 20
          maxLength: 2048
        tenantId:
          type: string
          minLength: 36
          maxLength: 36
        authType:
          type: string
          enum:
            - OAUTH2
      required:
        - secretArn
        - tenantId
        - authType
    dataEntityConfiguration:
      type: object
      properties:
        crawlPersonalDrives:
          anyOf:
            - type: boolean
            - type: string
              enum:
                - 'true'
```

```
            - 'false'
    filterConfiguration:
      type: object
      properties:
        inclusionUserEmailAddresses:
          type: array
          maxItems: 100
          items:
            type: string
            minLength: 1
            maxLength: 1024
        userFilterPath:
          type: string
          minLength: 1
          maxLength: 1024
        exclusionDriveItems:
          type: array
          maxItems: 100
          items:
            type: string
            minLength: 1
            maxLength: 1024
        inclusionDriveItems:
          type: array
          maxItems: 100
          items:
            type: string
            minLength: 1
            maxLength: 1024
        absoluteDateBefore:
          type: string
          description: 'ISO 8601 date-time format (e.g., 2024-12-31T23:59:59Z)'
        absoluteDateAfter:
          type: string
          description: 'ISO 8601 date-time format (e.g., 2024-12-31T23:59:59Z)'
        maxFileSizeInMegaBytes:
          type: string
    deletionProtectionConfiguration:
      type: object
      properties:
        enableDeletionProtection:
          anyOf:
            - type: boolean
            - type: string
```

```
            enum:
              - 'true'
              - 'false'
        deletionProtectionThreshold:
          type: string
          description: 'percentage value of range (0-100)'
    crawlIdentities:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - 'true'
            - 'false'
    accessControlConfiguration:
      type: object
      properties:
        crawlAcl:
          anyOf:
            - type: boolean
            - type: string
              enum:
                - 'true'
                - 'false'
    identityLoggingStatus:
      type: string
      enum:
        - ENABLED
        - DISABLED
  required:
    - connectionConfiguration
    - dataEntityConfiguration
    - type
```

Microsoft OneDrive YAML schema example for using the configuration property with AWS CloudFormation

The following is the Microsoft OneDrive YAML example for the Configuration property for CloudFormation:

```
configuration:
  type: ONEDRIVEV3
  crawlIdentities: false
  connectionConfiguration:
```

```
    secretArn: 'arn:aws:secretsmanager:us-west-2:123456789012:secret:my-one-drive-
secret'
    tenantId: '1234a12c-1234-1234-1abc-1234ab12a12a'
    authType: OAUTH2
  dataEntityConfiguration:
    crawlPersonalDrives: true
  accessControlConfiguration:
    crawlAcl: false
  filterConfiguration:
    inclusionUserEmailAddresses:
      - 'user123@amazon.com'
    maxFileSizeInMegaBytes: '50'
    exclusionDriveItems:
      - 'path/to/folder1'
      - 'path/to/file1'
    inclusionDriveItems:
      - 'path/to/folder2'
      - 'path/to/file2'
    userFilterPath: 's3://bucket/prefix/object.txt'
    absoluteDateBefore: '2025-08-02T00:00:00Z'
    absoluteDateAfter: '2025-08-01T00:00:00Z'
  deletionProtectionConfiguration:
    enableDeletionProtection: true
    deletionProtectionThreshold: '10'
  version: '3.0.0'
  identityLoggingStatus: DISABLED
```

How Amazon Q Business connector crawls Microsoft OneDrive ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

The Microsoft OneDrive connector for Amazon Q Business crawls files, including documents, spreadsheets, presentations, and notes, as the primary content type. It supports various file formats and integrates directly with Microsoft Office apps.

Roles/permissions: The Microsoft OneDrive connector translates Microsoft OneDrive permissions into ACLs that are compatible with Amazon Q Business. The basic permissions include:

- Read-only Access: users can view

- Preview Access: users can view but cannot download
- Edit: users can modify content

Permission Inheritance: The Microsoft OneDrive connector is designed to detect and handle hierarchical content organization. In Microsoft OneDrive files and subfolders inherit permissions from parent folders by default. Permissions can be customized at sub-folder and file levels. In this case, the ACLs are a union of the parent ACLs and child ACLs.

Identity Crawling: Domain-wide access is supported using service account authentication. Google Drive supports nested groups, meaning that one group can be a member of another. The connector handles complex group structures by flattening group memberships and ensuring that permissions are applied correctly across all levels.

Failure handling: The connector implements a fail-close approach, meaning that if there are permission-related issues or API failures, the document is skipped from ingestion rather than being made publicly accessible.

IAM role

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:{{secret_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/{{key_id}}"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
    },
    {
      "Sid": "AllowsAmazonQToCallPrincipalMappingAPIs",
      "Effect": "Allow",
```

```
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Microsoft OneDrive to Amazon Q Business (Original)

> **Note**
>
> **Original version notice:** This documentation covers the original version of the Microsoft OneDrive connector. For new implementations, we recommend using the new connector which offers improved performance. The original connector remains available for customers requiring specific features not yet supported in the new connector.

Limitations

When using the test data source connection feature, the Microsoft OneDrive connector has a potential issue when testing Identity Crawler. If it takes longer than five minutes, Amazon Q skips testing Identity Crawler, and moves on to the next test. Thus, it is possible for there to be a connection error with Identity Crawler even after finishing connection testing.

The Microsoft OneDrive original connector has the following known limitations:

- No support for syncing OneNote files
- When Access Control Lists (ACLs) are enabled, the "Sync only new or modified content" option is not available due to Microsoft OneDrive API limitations. We recommend using "Full sync" or "New, modified, or deleted content sync" modes instead, or disable ACLs if you need to use this sync mode.

Overview

The following table gives an overview of the Amazon Q Business Microsoft OneDrive original connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	OAuth 2.0 with Client Credentials Flow
	Authentication credentials	• Microsoft OneDrive Client ID

Category	Feature	Support
		• Microsoft OneDrive Client secret
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	No
	Entities	Yes. The following entities are supported: • File See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include/exclude using file path • Include/exclude using file name • Include/exclude using file type
	Sync mode	Supports full and incremental sync.
	File types	Supports all file types supported by Amazon Q.

Prerequisites

Before you begin, make sure that you have completed the following prerequisites.

In your Azure Active Directory (AD) application, make sure you have:

- Created an Azure Active Directory (AD) application.
- Used the AD application ID to register a secret key for the application on the AD site. The secret key must contain the client ID and a client secret.
- Copied the AD domain of the organization.
- Added the following Application API permissions to your AD application on the Microsoft Graph option:
  - Read files in all site collections (`Files.Read.All`)
  - Read all users' full profiles (`User.Read.All`)
  - Read all groups (`Group.Read.All`)

> **Note**
>
> Choose the Application permissions type instead of Delegated permissions while adding the API permissions.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Microsoft OneDrive authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Using the console

The following procedure outlines how to connect Amazon Q Business to Microsoft OneDrive using the original connector with the AWS Management Console.

Connecting Amazon Q to Microsoft OneDrive original connector

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Microsoft OneDrive** data source to your Amazon Q application.
5. Then, on the **Microsoft OneDrive** data source page, enter the following information:
6. In **Source**, enter the following information:

   - **OneDrive Tenant ID** Enter your OneDrive Tenant ID without the protocol. You can find your OneDrive Tenant ID under Directory ID in the Microsoft Entra ID (formerly Azure AD) admin center.

7. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
8. In **Authentication** – Choose between **New** and **Existing**.

   - If you choose **Existing**, select an existing secret for **Select secret**.

     If you choose **New**, enter the following information in the **New AWS Secrets Manager secret** section:

     i. **Secret name** – A name for your secret.

     ii. For **Client ID** and **Client secret** – Enter the authentication credential values from your OneDrive account and then choose **Save authentication**.

9. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

For more information, see VPC.

10. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

11. In **Sync scope**, for **Select OneDrive users**, choose between the following options:

- **Add a username file** – Choose to add a usernames file saved in an Amazon S3 bucket. Provide the path to the file by choosing **Browse**.

> **Note**
>
> If you choose this option, the IAM role for the data source must have read permissions for the Amazon S3 bucket where the file is stored.

- **Add usernames here** – You can add a maximum of 10 users using this option. To add more than 10 users, please create a file containing the usernames and choose **Add a user name file**.

12. For **Additional configuration – *optional***:

- For **Filter Patterns** – Add filter patterns to include or exclude certain files. You can add up to 100 patterns.

13. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

14. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

15. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
16. For **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New, modified, or deleted content sync** – Only sync new, modified, and deleted content.
17. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
18. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
19. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

20. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Microsoft OneDrive using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Microsoft OneDrive JSON schema

The following is the Microsoft OneDrive JSON schema:

```
{
```

```
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            }
          },
          "required": ["tenantId"]
        }
      }
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "email": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
```

```
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      },
      "attachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE","LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
```

```
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "calendar": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": [
```

```
            "fieldMappings"
          ]
        },
        "contacts": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": [
            "fieldMappings"
          ]
        },
        "notes": {
          "type": "object",
          "properties": {
            "fieldMappings": {
```

```
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": ["email"
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "inclusionPatterns": {
        "type": "array",
        "items": {
          "type": "string"
```

```
          }
        },
        "exclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionUsersList": {
          "type": "array",
          "items": {
            "type": "string",
            "format": "email"
          }
        },
        "exclusionUsersList": {
          "type": "array",
          "items": {
            "type": "string",
            "format": "email"
          }
        },
        "s3bucketName": {
          "type": "string"
        },
        "inclusionUsersFileName": {
          "type": "string"
        },
        "exclusionUsersFileName": {
          "type": "string"
        },
        "inclusionDomainUsers": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionDomainUsers": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "crawlCalendar": {
```

```
          "type": "boolean"
        },
        "crawlNotes": {
          "type": "boolean"
        },
        "crawlContacts": {
          "type": "boolean"
        },
        "crawlFolderAcl": {
          "type": "boolean"
        },
        "startCalendarDateTime": {
          "anyOf": [
            {
              "type": "string",
              "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
            },
            {
              "type": "string",
              "pattern": ""
            }
          ]
        },
        "endCalendarDateTime": {
          "anyOf": [
            {
            "type": "string",
            "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
            },
            {
              "type": "string",
              "pattern": ""
            }
          ]
        },
        "subject": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "emailFrom": {
          "type": "array",
          "items": {
```

```
            "type": "string",
            "format": "email"
          }
        },
        "emailTo": {
          "type": "array",
          "items": {
            "type": "string",
            "format": "email"
          }
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        }
      },
      "required": []
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "type" : {
      "type" : "string",
      "pattern": "ONEDRIVE"
    },
    "secretArn": {
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
```

```
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
connectionConfiguration	Configuration information for the endpoint for the data source.
repositoryEndpointMetadata	The endpoint information for the data source. This includes the tenant ID in the form of the OneDrive site URL.
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings. Specify the type of data source and the secret ARN.
secretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your OneDrive . The secret must contain a JSON structure with the following keys: `{ "clientID": "OAuth Client ID", "password": "client secret" }`
additionalProperties	Additional configuration options for your content in your data source.

Configuration	Description
`isCrawlAcl`	Specify `true` to crawl access control informati on from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.
• `userNameFilter` • `userFilterPath` • `inclusionFileTypePatterns` • `exclusionFileTypePatterns` • `inclusionFileNamePatterns` • `exclusionFileNamePatterns` • `inclusionFilePathPatterns` • `exclusionFilePathPatterns`	A collection of strings that specifies which entities to filter.
`isUserNameOnS3`	`true` to provide a list of user names in a file stored in an Amazon S3.
`type`	The type of data source. Specify `ONEDRIVE` as your data source type.

Configuration	Description
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

Configuration	Description
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index
`version`	The version of this template that's currently supported (1.0.0).

How Amazon Q Business connector crawls Microsoft OneDrive ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

The Microsoft OneDrive connector for Amazon Q Business crawls files, including documents, spreadsheets, presentations, and notes, as the primary content type. It supports various file formats and integrates directly with Microsoft Office apps.

Roles/permissions: The Microsoft OneDrive connector translates Microsoft OneDrive permissions into ACLs that are compatible with Amazon Q Business. The basic permissions include:

- Read-only Access: users can view

- Preview Access: users can view but cannot download
- Edit: users can modify content

Permission Inheritance: The Microsoft OneDrive connector is designed to detect and handle hierarchical content organization. In Microsoft OneDrive files and subfolders inherit permissions from parent folders by default. Permissions can be customized at sub-folder and file levels. In this case, the ACLs are a union of the parent ACLs and child ACLs.

Identity Crawling: Individual user and group synchronization is supported, including federated groups. Users and groups are synced using email IDs (each group in Active Directory will have email assigned to it).

Change Management: ACL changes are supported in Change Log Mode, ensuring that items added, updated, or deleted since the last crawl are indexed. Any changes to access or permissions of groups or users for any entity will be captured.

Failure handling: The connector implements a fail-close approach, meaning that if there are permission-related issues or API failures, the document is skipped from ingestion rather than being made publicly accessible.

Microsoft OneDrive data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved fields** – Mapped to reserved fields in the Amazon Q index that filter chat responses for your end users.
- **Custom fields** – Mapped to custom fields in the Amazon Q index. You can create custom fields when you create your application or data source. You can use custom fields to provide additional information to help your end users.

For more information, see Mapping data source fields.

The following table lists the Microsoft OneDrive data source connector entities and their associated attributes that you can map to Amazon Q index fields.

Entity	Attributes	Field type
File	• createdBy • createdDateTime • lastModifiedBy • lastModifiedDateTime • name • parentReference • size • webUrl	• String • Date • String • Date • String • String • Long • String

IAM role

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
```

```
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
```

```
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
```

```
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
```

```
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Error codes

The following table provides information about error codes you may see for the Microsoft OneDrive original connector and suggested resolutions.

Error code	Error message	Suggested resolution
OND-5000	Exception occurred while sending request to OneDrive api for testing	Try again.

Error code	Error message	Suggested resolution
	connection, please try again later.	
OND-5001	Provided client ID key is not Valid.	Provide a valid client ID.
OND-5002	Provided client secret key is not valid.	Provide valid client secret.
OND-5003	Provided tenant ID key is not valid.	Provide a valid tenant ID.
OND-5102	Client ID cannot be null/ empty.	Provide a valid client ID.
OND-5103	Tenant ID cannot be null/empty.	Provide a valid tenant Id.
OND-5104	Client Secret cannot be null/empty.	Provide a valid client Secret.
OND-5105	Invalid client ID pattern.	Provide a valid client ID.
OND-5106	Client Secret Over maximum length.	Length of client secret ID should be at least 256. Provide a valid client secret.
OND-5107	User Name Filter/ User Name Path should not be null or empty value.	Provide User Name Filter or User Name Path.
OND-5108	User Name Filter can only support up to 10 users.	Provide up to 10 users in User Name Filter or provide file of list of users in User Name Path.
OND-5109	Users mentioned in the list do not belong to the same domain.	Provide valid list of users which belong to same domain.

Error code	Error message	Suggested resolution
OND-5110	Users mentioned in the list are not valid.	Provide valid users.
OND-5200	Exception occurred while fetching files in full crawl.	Check logs for more details.
OND-5203	Exception occurred while fetching drive files.	Provide correct credentials.
OND-5204	Exception occurred while fetching OneNote files.	Check logs for more details.
OND-5300	Exception occurred while fetching files in change log.	Check logs for more details.
OND-5400	Exception occurred while building group details.	Check logs for more details.
OND-5401	Exception occurred while fetching list of groups.	Check logs for more details.
OND-5500	Exception occurred while getting file content response.	Check logs for more details.
OND-5501	Only String, String List, Date and Long formats are supported for field mappings.	Please provide valid formats in field mappings.
OND-5502	Exception occurred while fetching OneNote files.	Check logs for more details.

Connecting SharePoint (Online) to Amazon Q Business

Microsoft SharePoint is a collaborative website building service that lets you customize web content and create web pages, web sites, document libraries, and lists. You can connect SharePoint (Online) instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the SharePoint (Online) connector
- SharePoint (Online) connector overview
- Prerequisites for connecting Amazon Q Business to SharePoint (Online)
- Connecting Amazon Q Business to SharePoint (Online) using the console
- Connecting Amazon Q Business to SharePoint (Online) using APIs
- Connecting Amazon Q Business to SharePoint (Online) using AWS CloudFormation
- How Amazon Q Business connector crawls SharePoint (Online) ACLs
- SharePoint (Online) data source connector field mappings
- IAM role for SharePoint (Online) connector
- Understand error codes in the SharePoint (Online) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the SharePoint (Online) connector

The SharePoint (Online) connector has the following known limitations:

- The Amazon Q SharePoint (Online) connector supports custom field mappings only for the **Files** entity.

- If an entity name has a `%` character in its name, the connector will skip these files due to API limitations.
- OneNote can only be crawled by the connector using a Tenant ID, and with OAuth 2.0, OAuth 2.0 refresh token, or SharePoint (Online) App Only authentication activated for SharePoint (Online) Online.
- The connector crawls the first section of a OneNote document using its default name only, even if the document is renamed.
- The connector crawls event attachments only when **Events** is also selected as an entity to be crawled.
- The User Principal Name in your Azure Portal is a combination of upper case and lower case, the SharePoint (Online) API internally converts it to lower case. Because of this, the Amazon Q SharePoint (Online) connector sets ACL in lower case.

  For example, if **User principal name** is *`MaryMajor@domain.com`* in Azure portal, the ACL token in the SharePoint Connector will be *`marymajor@domain.com`*.
- When Access Control Lists (ACLs) are enabled, the "Sync only new or modified content" option is not available due to SharePoint (Online) API limitations. We recommend using "Full sync" or "New, modified, or deleted content sync" modes instead, or disable ACLs if you need to use this sync mode.
- If you want to crawl nested groups using **Identity crawler**, you have to activate Local as well as AD Group Crawling.
- To use **Identity Crawler** with SharePoint (Online) to crawl nested groups, you have to enable both Local and AD Group Crawling.
- Query responses based on AD Group ACLs are not supported for SharePoint (Online). You need to add users and groups directly to your document permissions list.
- Microsoft requires granting the "Sites.FullControl.All" permission to the application in order to ingest the source ACLs from SharePoint

SharePoint (Online) connector overview

The following table gives an overview of the Amazon Q Business SharePoint (Online) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	In order from most to least secure authentic ation type: • Microsoft Entra ID (formerly Azure AD) App-Only (OAuth 2.0 Certificate) (This is the preferred method of connection) • SharePoint App-Only with Client Credentials Flow • OAuth 2.0 with Resource Owner Password Flow • Basic authentication
	Authentication credentials	**Azure App-Only (OAuth 2.0 Certificate)** • Tenant ID • Certificate path • Client ID • Private key **SharePoint App-Only (OAuth 2.0 with Client Credentials Flow)** • Tenant ID • Microsoft Entra ID (formerly Azure AD) Client ID • Microsoft Entra ID (formerly Azure AD) Client secret • SharePoint App-Only Client ID • SharePoint App-Only Client secret **OAuth 2.0 with Resource Owner Password Flow**

Category	Feature	Support
		• SharePoint Tenant ID • SharePoint admin username • SharePoint admin password • Client ID • Client secret **Basic** • SharePoint (Online) admin username • SharePoint (Online) admin password
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Integration with Identity Provider (IdP)	Yes. Microsoft Entra ID (formerly Azure AD).
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	Yes. Supports custom metadata for **File** entity only.

Category	Feature	Support
	Entities	Yes. The following entities are supported: • Files • Attachments • Link • Pages • Events • Comments • List Data See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include/exclude by **Links** • Include/exclude by **Pages** • Include/exclude by **Events** • Include/exclude by file name • Include/exclude by file path • Include/exclude by file type • Include/exclude by **OneNote Section** name • Include/exclude by **OneNote Page** name
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Category	Feature	Support
	Crawled as a document	• Each event • Each page • Each file • Each link • Each file attachment • Each comment • Each OneNote

Prerequisites for connecting Amazon Q Business to SharePoint (Online)

The following page outlines the prerequisites you need to complete before connecting SharePoint (Online) to Amazon Q, based on the authentication mode of your choice.

> **Note**
>
> For more information on connecting SharePoint (Online) to Amazon Q Business, see Connect Amazon Q Business to Microsoft SharePoint Online using least privilege access controls and Find answers accurately and quickly using Amazon Q Business with the SharePoint Online connector in the *AWS Machine Learning Blog*.

Topics

- Prerequisites for using Microsoft Entra ID (formerly Azure AD) App-Only authentication
- Prerequisites for using OAuth 2.0 authentication
- Prerequisites for using SharePoint App-Only authentication
- Prerequisites for using basic authentication

Prerequisites for using Microsoft Entra ID (formerly Azure AD) App-Only authentication

If you're using Microsoft Entra ID (formerly Azure AD) App-Only authentication, make sure you've completed the following steps in SharePoint (Online):

- Copied your SharePoint (Online) instance URLs. The format for the host URL you enter is *`https://yourdomain.sharepoint.com/sites/mysite`* or *`https://yourcompany.sharepoint.com`*. Your URL must start with `https` and contain `sharepoint.com`.
- Copied the domain name of your SharePoint (Online) instance URL.
- Copied the tenant ID of your Microsoft SharePoint (Online) instance. For details on how to find your tenant ID, see Find your Microsoft 365 tenant ID on the Microsoft website.
- Generated an X.509 certificate. For more information on how to create and configure an X.509 certificate, see Granting access via Microsoft Entra ID (formerly Azure AD) App-Only and New-PnPAzureCertificate in *Microsoft developer documentation*.
- After generating the X.509 certificate, upload your .CRT file (the public certificate) to an Amazon S3 bucket. Note the file path to a X.509 certificate you have created and stored in an Amazon S3 bucket. (Ex. `s3://bucket-name/path/to/certificate.crt`). Ensure that your Amazon Q Business IAM role has permissions to read from this Amazon S3 bucket.
- Noted the private key and the Client ID you generated after SharePoint (Online) Azure App registration.
- Configured a Sharepoint (Online) Azure App using one of the two options below and noted its Client ID and Client secret.

> **Note**
>
> If you want to crawl specific sites, you can choose to restrict permissions to specific sites rather than all sites available in the domain. To do this, use the Sites.Selected (Application) permission. With this API permission, you need to set access permission on every site explicitly through the Microsoft Graph API. For more information, see Microsoft's blog on Sites.Selected permissions.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.

- Stored your SharePoint (Online) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Microsoft Entra ID (formerly Azure AD) App-Only Option 1: Global Read Access

If you anticipate that you will be indexing several Sharepoint sites and would like to simplify your setup process, you can take the following steps to provide the Q Business Sharepoint connector global access. Otherwise, skip to section 2 below.

1. Create a Sharepoint client app to which we will assign the permissions needed by your Q Business connector. To register the app:

    a. Log in to the Azure Portal with your Microsoft account.

    b. i. Provide the name for your application. In the example we are using the name TargetApp. The Amazon Q Business application uses TargetApp to connect to the SharePoint Online site to crawl and index the data.

    ii. Choose "Accounts" in the organizational directory. (Tenant name only - Single tenant).

    iii. Choose "Register".

    iv. Note down the application (client ID and the directory (tenant) on the Overview page, as you'll need them when prompted for "TargetApp-ClientId" and "TenantId".

    v. Navigate to "Manage > API Permissions" in the navigation pane

    vi. Navigate to "Add a permission > Sharepoint > Application permissions" to allow the application to read data in your organization's directory regarding the signed-in user.

    vii. Search "AllSites.Read".

    viii. Choose "Add permissions".

    ix. Navigate to "Add a permission > Microsoft Graph > Application permissions"

    x. Search and add the following permissions:

- "Notes.Read.All"
- "Sites.Read.All"
- "Sites.FullControl.All (Application)" (required only if you intend to enable ACLs)
- "Sites.Read.All (Application)"(required only if you intend to enable ACLs)
- "Sites.FullControl.All" (required only if you intend to enable ACLs)
- "GroupMember.Read.All" (required only if you intend to enable ACLs)
- "User.Read.All" (required only if you intend to enable ACLs)

xi. Navigate to "Remove permission"

xii. Remove the original "User.Read - Delegated" permission

xiii. Choose "Grant admin consent" for the default directory

xiv. Save the client ID generated from this app for when you configure the Sharepoint connector in the Q Business console or API

The following tables summarize all the permissions your application should have.

- If you're not using ACL, your application should have the permission:

Microsoft Graph	Sharepoint
Notes.Read.All (Application) – Read all OneNote notebooks	AllSites.Read (Delegated) - Read items in all site collections
Sites.Read.All (Application) - Read items in all site collections	

> **Note**
>
> Read.All and Sites.Read.All are required only if you want to crawl OneNote Documents.

- If you're using ACL, your application should have the following permissions:

Microsoft Graph	Sharepoint
GroupMember.Read.All (Application) – Read all group memberships	AllSites.Read (Delegated) – Read items in all site collections
Notes.Read.All (Application) – Read all OneNote notebooks	
Sites.FullControl.All (Application) – Have full control of all site collections	
Sites.Read.All (Application) – Read items in all site collections	
User.Read.All (Application) – Read all users' full profiles	

2. Create a client secret for your Sharepoint App:

    a. Within your client App navigate to "Clients and secrets > Client secrets"

    b. Click on create a new secret.

3. Generate a new Certificate to be shared between Q Business SharePoint Connector and Microsoft Entra ID (formerly Azure AD) App:

    a. Use the example command below to generate your own x509 certificate.

    b. Run the following command:`openssl req -x509 -newkey rsa:2048 -noenc -sha1 -keyout /tmp/private.key -out /tmp/sharepoint.crt -nodes -set_serial 1 -days 365 -subj "/CN=amazon/emailAddress=example@aws.com/C=US/ST=Texas/L=Dallas/O=amazon/OU=amazon`

    c. Save the generated private key located in /tmp/private.key for later when you configure the Q Business Sharepoint connector via the Q Business console or API.

Microsoft Entra ID (formerly Azure AD) App-Only Option 2: Read Access for only Selected Sites

If you anticipate that you will be indexing a manageable number of Sharepoint sites and would prefer to limit the permissions of the Q Business connector to just the Sharepoint sites you intend to index, you can take the following steps:

1. Create a Sharepoint client app: Create a Sharepoint client app to which we will assign the permissions needed by your Q Business connector. To register the app:

    a. Log in to the Azure Portal with your Microsoft account.

    b. Choose "New Registration":

        i. Provide the name for your application. In the example we are using the name TargetApp. The Amazon Q Business application uses TargetApp to connect to the SharePoint Online site to crawl and index the data.

        ii. Choose "Accounts" in the organizational directory. (Tenant name only - Single tenant).

        iii. Choose "Register".

        iv. Note down the application (client ID and the directory (tenant) on the Overview page, as you'll need them when prompted for "TargetApp-ClientId" and "TenantId".

        v. Navigate to "Manage > API Permissions" in the navigation pane

        vi. Navigate to "Add a permission > Sharepoint > Application permissions" to allow the application to read data in your organization's directory regarding the signed-in user.

        vii. Search "Sites.Selected".

        viii. Choose "Add permissions".

        ix. Navigate to "Add a permission > Microsoft Graph > Application permissions"

        x. Search and add the following permissions:

            - "Notes.Read.All"
            - "Sites.Selected"
            - "GroupMember.Read.All" (required only if you intend to enable ACLs)
            - "User.Read.All" (required only if you intend to enable ACLs)

        xi. Navigate to "Remove permission"

        xii. Remove the original "User.Read - Delegated" permission

        xiii. Choose "Grant admin consent" for the default directory

        xiv. Save the client ID generated from this app for when you configure the Sharepoint connector in the Q Business console or API

The following tables summarize all the permissions your application should have.

- If you're not using ACL, your application should have the permissions:

Microsoft Graph	Sharepoint
Notes.Read.All (Application) – Read all OneNote notebooks	AllSites.Read (Delegated) - Read items in all site collections
Site.Read.All (Application) - Read items in all site collections	

> **Note**
>
> Read.All and Sites.Read.All are required only if you want to crawl OneNote Documents.

- If you're using ACL, your application should have the following permissions:

Microsoft Graph	Sharepoint
GroupMember.Read.All (Application) – Read all group memberships	AllSites.Read (Delegated) – Read items in all site collections
Notes.Read.All (Application) – Read all OneNote notebooks	
Sites.FullControl.All (Application) – Have full control of all site collections	
Sites.Read.All (Application) – Read items in all site collections	
User.Read.All (Application) – Read all users' full profiles	

Sites.Selected - Have control of selected sites	

2. Create a client secret for your Sharepoint App:

    a. Within your client App navigate to "Clients and secrets > Client secrets"

    b. Click on create a new secret.

3. Generate a new Certificate to be shared between Q Business SharePoint Connector and Microsoft Entra ID (formerly Azure AD) App:

    a. Run the following command: `openssl req -x509 -newkey rsa:2048 -noenc -sha1 -keyout /tmp/private.key -out /tmp/sharepoint.crt -nodes -set_serial 1 -days 365 -subj "/CN=amazon/emailAddress=example@aws.com/C=US/ST=Texas/L=Dallas/O=amazon/OU=amazon"`

    b. Save the generated private key located in /tmp/private.key for later when you configure the Q Business Sharepoint connector via the Q Business console or API.

    c. Upload the generated certificate located in /tmp/sharepoint.crt to an S3 bucket so you can use it later when you configure the Q Business Sharepoint connector via the Q Business console or API. You will also need this certificate for the next step.

4. Update your Sharepoint Client App’s Certificate:

    a. Navigate to the Sharepoint client app you created in step 1.

    b. Navigate to “Certificates and secrets > Certificates > Upload certificate” and upload the certificate (.crt file) you generated in step 4.

5. Create a Sharepoint admin app: This app will be used to provide the necessary site read permissions for the client OAuth App you created in the previous step. You can delete this admin app after you have completed all the steps. To register the app:

    a. Log in to the Azure Portal with your Microsoft account.

    b. Choose “New Registration”:

        i. Provide the name for your application.

        ii. Choose "Accounts" in the organizational directory. (Tenant name only - Single tenant).

        iii. Choose "Register".

iv. Locate your app ID, app secret, and tenant ID for your admin app and save them for the next step.

v. Navigate to "Manage > API Permissions" in the navigation pane

vi. Navigate to "Add a permission > Sharepoint > Application permissions" to allow the application to read data in your organization's directory regarding the signed-in user.

vii. Search "Sites.FullControl.All".

viii. Choose "Add permissions".

ix. Navigate to "Add a permission > Microsoft Graph > Application permissions"

x. Search "Sites.Read.All".

xi. Choose "Add permissions".

6. Generate an access token for your Sharepoint admin app: Now use the following code snippet to generate an access token for your app, but replace adminAppID, adminAppSecret, and tenantID with the values you saved from step 2.

```
adminAppId=$1
adminAppSecret=$2
tenantId=$3

tokenResponse=$(curl -s --location \
"https://login.microsoftonline.com/$tenantId/oauth2/v2.0/token" \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode "grant_type=client_credentials" \
--data-urlencode "client_id=$adminAppId" \
--data-urlencode "client_secret=$adminAppSecret" \
--data-urlencode "scope=offline_access https://graph.microsoft.com/.default")

adminAppToken=$(echo $tokenResponse | jq -r '.access_token')
echo $adminAppToken
```

7. Obtain a Site ID for each of your Sharepoint sites: Repeat the following steps for each of the Sharepoint sites you want your Q Business connector to crawl:

a. Visit `https://{yourcompany}.sharepoint.com/sites/{SiteName}`in a browser. Enter the appropriate login credentials if needed. Validate that you are able to see your SharePoint site

b. Now append /_api/site/id at the end of {SiteName}. You should see a response something similar to below containing your site id (96a47524-4b21-446f-bf96-96d2f6fe4aa7)

```
<d:Id m:type="Edm.Guid" xmlns:d="http://schemas.microsoft.com/ado/2007/08/
dataservices" xmlns:georss="http://www.georss.org/georss" xmlns:gml="http://
www.opengis.net/gml" xmlns:m="http://schemas.microsoft.com/ado/2007/08/
dataservices/metadata">96a47524-4b21-446f-bf96-96d2f6fe4aa7</d:Id>
```

8. Grant your Sharepoint client app permissions to your selected sites: Now that you have created your Sharepoint admin app, Sharepoint client app, and have a list of site ids, you are ready to grant your client app the necessary permissions to access these sites. Repeat the following steps for each of the site ids you obtained from step 4.

   a. Modify the code snippet below to provide the following:

      i. clientAppId: The Application (client) ID from step 1.

      ii. clientAppName: The display name of your Sharepoint client app from step 1.

      iii. adminToken: The access token you generated in step 6.

      iv. siteId: One of the site ids you obtained from step 7.

   b. Run the following command:

```
clientAppId=$1
clientAppName=$2
clientAppId=$1
clientAppName=$2
adminToken=$3
siteToGivePermissionTo=$4

grantPermissionResponse=$(curl -s --location "https://graph.microsoft.com/v1.0/
sites/$siteToGivePermissionTo/permissions" \
    --header "Content-Type: application/json" \
    --header "Authorization: Bearer $adminToken" \
    --data '{
         "roles": ["fullcontrol"],
         "grantedToIdentities": [{
            "application": {
              "id": "'${clientAppId}'",
              "displayName": "'${clientAppName}'"
            }
          }]
        }')

echo $grantPermissionResponse
```

c. If the command was successful, you'll see a response as follows:


```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/
$metadata#sites('awsplatodemo.sharepoint.com%2C96a47524-4b21-446f-
bf96-96d2f6fe4aa7')/permissions/$entity",
  "id":
 "aTowaS50fG1zLnNwLmV4dHxjMDY5YjhlMi03NGFhLTQzZTQtODljYi1kNmZkMzU4ZmVjZThAZjIwNDQ2OTItZ
  "roles": [
    "fullcontrol"
  ],
  "grantedToIdentitiesV2": [
    {
      "application": {
        "displayName": "demo-client-app",
        "id": "c069b8e2-74aa-43e4-89cb-d6fd358fece8"
      }
    }
  ],
  "grantedToIdentities": [
    {
      "application": {
        "displayName": "demo-client-app",
        "id": "c069b8e2-74aa-43e4-89cb-d6fd358fece8"
      }
    }
  ]
}
```


Prerequisites for using OAuth 2.0 authentication

If you're using OAuth 2.0 authentication, make sure you've completed the following steps in SharePoint (Online):

- Copied your SharePoint (Online) instance URLs. The format for the host URL you enter is *`https://yourdomain.sharepoint.com/sites/mysite`* or *`https://yourcompany.sharepoint.com`*. Your URL must start with `https` and contain `sharepoint.com`.
- Copied the domain name of your SharePoint (Online) instance URL.

- Copied the tenant ID of your Microsoft SharePoint (Online) instance. For details on how to find your tenant ID, see Find your Microsoft 365 tenant ID on the Microsoft website.
- Noted the username and password that you use to connect to SharePoint (Online).
- Noted the Client ID and Client secret generated after SharePoint (Online) Azure App registration.
- Deactivate multi-factor authentication (MFA) in your SharePoint account, so that Amazon Q is not blocked from crawling your SharePoint content.
- Configured a Sharepoint (Online) Azure App using one of the two options below and noted its Client ID and Client secret.

OAuth2.0 Option 1: Global Read Access

If you anticipate that you will be indexing several Sharepoint sites and would like to simplify your setup process, you can take the following steps to provide the Q Business Sharepoint connector global access. Otherwise, skip to section 2 below.

To register the app:

1. Log in to the Azure Portal with your Microsoft account.
2. Choose "New Registration":
    a. Provide the name for your application. In the example we are using the name TargetApp. The Amazon Q Business application uses TargetApp to connect to the SharePoint Online site to crawl and index the data.
    b. Choose "Accounts" in the organizational directory. (Tenant name only - Single tenant).
    c. Choose "Register".
    d. Note down the application (client ID and the directory (tenant) on the Overview page, as you'll need them when prompted for "TargetApp-ClientId" and "TenantId".
    e. Navigate to "Manage > API Permissions" in the navigation pane
    f. Navigate to "Add a permission > Sharepoint > Application permissions" to allow the application to read data in your organization's directory regarding the signed-in user.
    g. Search "AllSites.Read".
    h. Choose "Add permissions".
    i. Navigate to "Add a permission > Microsoft Graph > Application permissions"
    j. Search and add the following permissions:

- "Notes.Read.All"
- "Sites.Read.All"
- "Sites.FullControl.All" (required only if you intend to enable ACLs)
- "GroupMember.Read.All" (required only if you intend to enable ACLs)
- "User.Read.All" (required only if you intend to enable ACLs)

k. Navigate to "Remove permission".

l. Remove the original "User.Read - Delegated" permission.

m. Choose "Grant admin consent" for the default directory.

n. Save the client ID generated from this app for when you configure the Sharepoint connector in the Q Business console or API.

The following tables summarize all the permissions your application should have.

- If you're not using ACL, your application should have the permissions:

Microsoft Graph	Sharepoint
Notes.Read.All (Application) – Read all OneNote notebooks	AllSites.Read (Delegated) - Read items in all site collections
Site.Read.All (Application) - Read items in all site collections	

> **Note**
>
> Note.Read.All and Sites.Read.All are required only if you want to crawl OneNote Documents.

- If you're using ACL, your application should have the following permissions:

Microsoft Graph	Sharepoint
GroupMember.Read.All (Application) – Read all group memberships	AllSites.Read (Delegated) – Read items in all site collections

Notes.Read.All (Application) – Read all OneNote notebooks	
Sites.FullControl.All (Application) – Have full control of all site collections	
Sites.Read.All (Application) – Read items in all site collections	
User.Read.All (Application) – Read all users' full profiles	

> **Note**
>
> GroupMember.Read.All and User.Read.All are required only if Identity crawler is activated.

3. Create a client secret for your Sharepoint App:

    a. Within your client App navigate to "Clients and secrets > Client secrets"

    b. Click on create a new secret.

OAuth2.0 Option 2: Read Access Only for Selected Sites

For organizations planning to index a manageable number of Sharepoint sites with limited permissions, the following steps provide the necessary setup:

1. Create a Sharepoint client app for OAuth: Now create a Sharepoint client OAuth app to which we will assign the permissions needed by your Q Business connector. To register the app:

    a. Log in to the Azure Portal with your Microsoft account.

    b. Choose "New Registration":

        i. Provide the name for your application. In the example we are using the name TargetApp. The Amazon Q Business application uses TargetApp to connect to the SharePoint Online site to crawl and index the data.

        ii. Choose "Accounts" in the organizational directory. (Tenant name only - Single tenant).

iii. Choose "Register".

iv. Note down the application (client ID and the directory (tenant) on the Overview page, as you'll need them when prompted for "TargetApp-ClientId" and "TenantId".

v. Navigate to "Manage > API Permissions" in the navigation pane

vi. Navigate to "Add a permission > Sharepoint > Application permissions" to allow the application to read data in your organization's directory regarding the signed-in user.

vii. Search "Sites.Selected".

viii. Choose "Add permissions".

ix. Navigate to "Add a permission > Microsoft Graph > Application permissions"

x. Search and add the following permissions:

- "Notes.Read.All"
- "Sites.Selected"
- "GroupMember.Read.All" (required only if you intend to enable ACLs)
- "User.Read.All" (required only if you intend to enable ACLs)

xi. Navigate to "Remove permission"

xii. Remove the original "User.Read - Delegated" permission

xiii. Choose "Grant admin consent" for the default directory

xiv. Save the client ID generated from this app for when you configure the Sharepoint connector in the Q Business console or API

The following tables summarize all the permissions your application should have.

- If you're not using ACL, your application should have the permissions:

Microsoft Graph	Sharepoint
Notes.Read.All (Application) – Read all OneNote notebooks	Sites.Selected (Application) - Read items in selected site collections
Sites.Selected (Application) - Read items in selected site collections	

> **Note**
>
> Note.Read.All and Sites.Read.All are required only if you want to crawl OneNote Documents.

- If you're using ACL, your application should have the following permissions:

Microsoft Graph	Sharepoint
GroupMember.Read.All (Application) – Read all group memberships	AllSites.Read (Delegated) – Read items in all site collections
Notes.Read.All (Application) – Read all OneNote notebooks	
Sites.FullControl.All (Application) – Have full control of all site collections	
Sites.Read.All (Application) – Read items in all site collections	
User.Read.All (Application) – Read all users' full profiles	

> **Note**
>
> Note. GroupMember.Read.All and User.Read.All are required only if Identity crawler is activated.

2. Create a client secret for your Sharepoint App:

   a. Within your client App navigate to "Clients and secrets > Client secrets"

   b. Click on create a new secret.

3. Create a Sharepoint admin app: This app will be used to provide the necessary site read permissions for the client OAuth App you created in the previous step. You can delete this admin app after you have completed all the steps. To register the app:

a. Log in to the Azure Portal with your Microsoft account.

b. Choose "New Registration":

i. Provide the name for your application.

ii. Choose "Accounts" in the organizational directory. (Tenant name only - Single tenant).

iii. Choose "Register".

iv. Locate your app ID, app secret, and tenant ID for your admin app and save them for the next step.

v. Navigate to "Manage > API Permissions" in the navigation pane

vi. Navigate to "Add a permission > Sharepoint > Application permissions" to allow the application to read data in your organization's directory regarding the signed-in user.

vii. Search "Sites.FullControl.All".

viii. Choose "Add permissions".

ix. Navigate to "Add a permission > Microsoft Graph > Application permissions"

x. Search "Sites.Read.All".

xi. Choose "Add permissions".

4. Generate an access token for your Sharepoint admin app: Now use the following code snippet to generate an access token for your app, but replace adminAppID, adminAppSecret, and tenantID with the values you saved from step 2.

```
adminAppId=$1
adminAppSecret=$2
tenantId=$3

tokenResponse=$(curl -s --location \
"https://login.microsoftonline.com/$tenantId/oauth2/v2.0/token" \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode "grant_type=client_credentials" \
--data-urlencode "client_id=$adminAppId" \
--data-urlencode "client_secret=$adminAppSecret" \
--data-urlencode "scope=offline_access https://graph.microsoft.com/.default")

adminAppToken=$(echo $tokenResponse | jq -r '.access_token')
echo $adminAppToken
```

5. Obtain a Site ID for each of your Sharepoint sites: Repeat the following steps for each of the Sharepoint sites you want your Q Business connector to crawl:

   a. Visit https://{yourcompany}.sharepoint.com/sites/{SiteName} in a browser. Enter the appropriate login credentials if needed. Validate that you are able to see your SharePoint site

   b. Now append /_api/site/id at the end of {SiteName}. You should see a response something similar to below containing your site id ([IP_ADDRESS]a7)

```
<d:Id m:type="Edm.Guid" xmlns:d="http://schemas.microsoft.com/ado/2007/08/
dataservices" xmlns:georss="http://www.georss.org/georss" xmlns:gml="http://
www.opengis.net/gml" xmlns:m="http://schemas.microsoft.com/ado/2007/08/
dataservices/metadata">[IP_ADDRESS]a7</d:Id>
```

6. Grant your Sharepoint client app permissions to your selected sites: Now that you have created your Sharepoint admin app, Sharepoint client app, and have a list of site ids, you are ready to grant your client app the necessary permissions to access these sites. Repeat the following steps for each of the site ids you obtained from step 4.

   a. Modify the code snippet below to provide the following:

      i. clientAppId: The Application (client) ID from step 1

      ii. clientAppName: The display name of your Sharepoint client app from step 1

      iii. adminToken: The adminAppToken you generated in step 3

      iv. siteId: One of the site ids you obtained from step 4.

   b.

```
clientAppId=$1
clientAppName=$2
adminToken=$3
siteToGivePermissionTo=$4

grantPermissionResponse=$(curl -s --location "https://graph.microsoft.com/v1.0/
sites/$siteToGivePermissionTo/permissions" \
--header "Content-Type: application/json" \
--header "Authorization: Bearer $adminToken" \
--data '{
"roles": ["fullcontrol"],
"grantedToIdentities": [{
"application": {
"id": "'${clientAppId}'",
"displayName": "'${clientAppName}'"
```

```
}
}]
}')

echo $grantPermissionResponse
```

c. If the command was successful, you'll see a response as follows:

```
{
"@odata.context": "https://graph.microsoft.com/v1.0/
$metadata#sites('awsplatodemo.sharepoint.com%2C[IP_ADDRESS]a7')/permissions/
$entity",
"id":
 "aTowaS50fG1zLnNwLmV4dHxjMDY5YjhlMi03NGFhLTQzZTQtODljYi1kNmZkMzU4ZmVjZThAZjIwNDQ2OTItZ
"roles": [
"fullcontrol"
],
"grantedToIdentitiesV2": [
{
"application": {
"displayName": "demo-client-app",
"id": "c069b8e2-74aa-43e4-89cb-d6fd358fece8"
}
}
],
"grantedToIdentities": [
{
"application": {
"displayName": "demo-client-app",
"id": "c069b8e2-74aa-43e4-89cb-d6fd358fece8"
}
}
]
}
```

Prerequisites for using SharePoint App-Only authentication

If you're using SharePoint App-Only authentication, make sure you've completed the following steps in SharePoint (Online):

- Copied your SharePoint (Online) instance URLs. The format for the host URL you enter is *https://yourdomain.sharepoint.com/sites/mysite* or *https://*

yourcompany.sharepoint.com. Your URL must start with `https` and contain `sharepoint.com`.

- Copied the domain name of your SharePoint (Online) instance URL.
- Copied the tenant ID of your Microsoft SharePoint (Online) instance. For details on how to find your tenant ID, see Find your Microsoft 365 tenant ID on the Microsoft website.
- Noted your SharePoint (Online) client ID and client secret generated while granting permission to SharePoint App-Only, and your Client ID and Client secret generated after SharePoint (Online) Azure App registration.
- **If you're crawling OneNote documents and using Identity crawler**, added the following permissions:

Microsoft Graph
• GroupMember.Read.All (Application) – Read all group memberships • Notes.Read.All (Application) – Read all OneNote notebooks • Sites.Read.All (Application) – Read items in all site collections • User.Read.All (Application) – Read all users' full profiles

> **Note**
>
> No API permissions are required for crawling entities using SharePoint (Online) **App-Only authentication**.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.

- Stored your SharePoint (Online) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Prerequisites for using basic authentication

If you're using basic authentication, make sure you've completed the following steps in SharePoint (Online):

- Copied your SharePoint (Online) instance URLs. The format for the host URL you enter is *`https://yourdomain.sharepoint.com/sites/mysite`* or *`https://yourcompany.sharepoint.com`*. Your URL must start with `https` and contain `sharepoint.com`.
- Copied the domain name of your SharePoint (Online) instance URL.
- Noted your basic authentication credentials containing the username and password that you use to connect to SharePoint (Online) Online.
- Deactivated **Security Defaults** in your Azure portal using an administrative user. For more information on managing security default settings in the Azure portal, see Microsoft documentation on how to enable/disable security defaults.
- Deactivated multi-factor authentication (MFA) in your SharePoint account, so that Amazon Q is not blocked from crawling your SharePoint content.

> **Note**
>
> No API permissions are required for crawling entities using **Basic authentication**.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your SharePoint (Online) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to SharePoint (Online) using the console

The following procedure outlines how to connect Amazon Q Business to SharePoint (Online) using the AWS Management Console.

Connecting Amazon Q to SharePoint (Online)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **SharePoint** data source to your Amazon Q application.
5. Then, on the **SharePoint (Online)** data source page, enter the following information:
6. **Name and description**, do the following:

- For **Data source name** – Name your data source for easy tracking.

> **Note**
>
> You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. In **Source**, enter the following information:

   a. In **Source**, for **Hosting Method** – Choose **SharePoint Online**.

   b. **Site URLs specific to your SharePoint repository** – Enter the SharePoint host URLs. The format for the host URLs you enter is *`https://yourcompany.sharepoint.com/sites/mysite`* or *`https://yourcompany.sharepoint.com`*. The URL must start with `https` protocol. Separate URLs with a new line. You can add up to 100 URLs.

   c. **Domain** – Enter the SharePoint domain. For example, the domain in the URL *`https://yourdomain.sharepoint.com/sites/mysite`* is *`yourdomain`*. Note that the domain name in the URL and the domain name you're expected to enter in the domain field can be different.

8. **Authorization** – Choose whether Amazon Q will crawl user and group access control list (ACL) information from your data source. Amazon Q can use this information to only generate responses from documents your end users have access to. You can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

> **Note**
>
> Using ACL data to filter responses is not a replacement for user authentication and authorization for your application. For information on setting up identity management for Amazon Q, see Integrating with an Identity Provider (IdP).

> **Important**
>
> If you don't specify a value, **Email** is considered as the default value.

9. For **Authentication**, choose between **Basic**, **Oauth 2.0**, **Azure AD App-Only authentication**, and **SharePoint App-Only authentication** based on your use case.

> **Note**
>
> OneNote can only be crawled by the connector using a Tenant ID, and with OAuth 2.0, or SharePoint (Online) App Only authentication activated.

a. If using **Microsoft Entra ID (formerly Azure AD) App-Only authentication**, enter the following information:

- **Tenant ID** – Tenant ID of your SharePoint account. To learn how to find your Tenant ID, see Get subscription and tenant IDs in the Azure portal in Azure portal documentation.
- **Microsoft Entra ID (formerly Azure AD) self-signed X.509 certificate** – Certificate to authenticate the connector for Microsoft Entra ID (formerly Azure AD). For more information on how to do this, see Granting access via Microsoft Entra ID (formerly Azure AD) App-Only and New-PnPAzureCertificate in *Microsoft developer documentation*.
- **Generate a certificate using OpenSSL** – As an example:

```
openssl req -x509 -newkey rsa:2048 -nodes -keyout /path/to/folder/private.key
 -out /path/to/folder/sharepoint.crt -days 365 -subj "/CN=ExampleCorp/
emailAddress=example@domain.com
/C=US/ST=Texas/L=Dallas/O=ExampleCorp/OU=IT" -set_serial 1
```

> **Note**
>
> Avoid using the -sha1 flag when generating certificates. SHA-1 is considered insecure and deprecated. Most modern browsers and systems reject certificates

signed with SHA-1. By default, OpenSSL uses a secure algorithm such as SHA-256 when the -sha1 flag is omitted.

- For **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your SharePoint authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens. Enter the following information in the window:
  - **Secret name** – A name for your secret.
  - **Client ID** – The Client ID generated when you complete Azure App registration for SharePoint (Online) in Entra ID.
  - **Private key** – A private key to authenticate the connector for Microsoft Entra ID (formerly Azure AD).
  - **Register a new app in the Microsoft Azure portal**:
    1. Log in to the Azure Portal with your Microsoft account.
    2. Choose New Registration:
       a. Provide the name for your application. In the example we are using the name `TargetApp`. The Amazon Q Business application uses TargetApp to connect to the SharePoint Online site to crawl and index the data.
       b. Choose "Accounts" in the organizational directory. (`Tenant name` only - Single tenant).
       c. Choose "Register".
       d. Note down the application (client ID and the directory (tenant) on the Overview page, as you'll need them when prompted for "TargetApp-ClientId" and "TenantId".
       e. Choose API permissions under "Manage" in the navigation pane.
       f. Choose "Add a permission" to allow the application to read data in your organization's directory regarding the signed-in user.
       g. Choose "Sharepoint".
       h. Choose "Application permissions".
       i. Choose "Sites.FullControl.All" from the User section.
       j. Choose "Add permissions".
    3. On the options menu, choose to "Remove" a permssion.
    4. Remove the original `User.Read - Delegated` permission.

5. Choose "Grant admin content" for the Default Directory.

b. If using **SharePoint App-Only authentication**, enter the following information:

- **Tenant ID**–Tenant ID of your SharePoint account. To learn how to find your Tenant ID, see Get subscription and tenant IDs in the Azure portal in Azure portal documentation.
- For **AWS Secrets Manager secret** — Choose an existing secret or create a Secrets Manager secret to store your SharePoint authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens. Enter the following information in the window:
  - **Secret name** – A name for your secret.
  - **SharePoint client ID** – The SharePoint client ID you generated when you registered App-Only at Tenant Level. ClientID format is *`ClientID@TenantId`*. For example, *`ffa956f3-8f89-44e7-b0e4-49670756342c@888d0b57-69f1-4fb8-957f-e1f0bedf82fe.`*
  - **SharePoint client secret** – The SharePoint client secret generated when your register for App-Only at Tenant Level.
  - **Client ID** – The Microsoft Entra ID (formerly Azure AD) client ID generated when you register SharePoint in Microsoft Entra ID (formerly Azure AD).
  - **Client secret** – The Microsoft Entra ID (formerly Azure AD) client secret generated when you register SharePoint to Microsoft Entra ID (formerly Azure AD).

c. If using **OAuth 2.0 authentication**, you must disable MFA in SharePoint. This is not recommended, but if you choose to use OAuth 2.0 authentication anyway, enter the following information:

- **Tenant ID** – Tenant ID of your SharePoint account. To learn how to find your Tenant ID, see Get subscription and tenant IDs in the Azure portal in Azure portal documentation.
- For **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your SharePoint authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens. Enter the following information in the window:
  - **Secret name** – A name for your secret.
  - **Username** – Username for your SharePoint account.
  - **Password** – Password for your SharePoint account.

- **Client ID** – The Client ID generated when you complete Azure App registration for SharePoint (Online) in Entra ID.
- **Client secret** – The Client secret generated when you complete Azure App registration for SharePoint (Online) in Entra ID.

d. If using **Basic Authentication**, you must disable MFA in SharePoint. This is not recommended, but if you choose to use Basic Auth anyway, enter the following information:

- For **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your SharePoint authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens. Enter the following information in the window:
  - **Secret name** – A name for your secret.
  - **Username** – Username for your SharePoint account.
  - **Password** – Password for your SharePoint account.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

The SharePoint connector supports Microsoft Entra ID (formerly Azure AD) groups associated with documents. In order for Microsoft Entra ID (formerly Azure AD) group members to search the data, you have to integrate Microsoft Entra ID (formerly Azure AD) with IAM Identity Center.

1. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

2. In **Sync scope**, choose from the following options :

   a. **Select entities** – Choose the entities that you want to crawl. You can select to crawl **All** entities or any combination of **Files**, **Attachments**, **Links**, **Pages**, **Events**, **Comments**, and **List Data**.

   b. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

   c. In **Additional configuration – *optional***, for **Entity regex patterns** – Add regular expression patterns for **Links**, **Pages**, and **Events** to include specific entities instead of syncing all your documents.

   d. In **Additional configuration**, for **Regex patterns** – Add regular expression patterns to include or exclude files by **File path**, **File name**, **File type**, **OneNote section name**, and **OneNote page name** instead of syncing all your documents. You can add up to 100 patterns.

   > **Note**
   >
   > Any valid regex pattern is supported. For example, if you use the regex `^QBusiness*`, any content starting with the word `QBusiness` followed by any number of characters will be filtered (`QBusiness_doc1` or `QBusiness`, but not `doc1_QBusiness`).

   > **Note**
   >
   > OneNote crawling is available only for OAuth 2.0 and SharePoint App Only authentication.

e. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

To extract audio transcriptions and video content, enable processing for the following file types:

f. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

3. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

- **Full sync** – Sync all content regardless of the previous sync status.
- **New or modified content sync** – Sync only new and modified documents.
- **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

For more details, see Sync mode.

4. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
5. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
6. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

7. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to SharePoint (Online) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- SharePoint (Online) configuration properties
- SharePoint (Online) JSON schema
- SharePoint (Online) JSON schema example

SharePoint (Online) configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-properties. • `siteUrls` • `domain` • `repositoryAdditionalProperties` • `tenantId`	Yes
`tenantId`	The tenant id of your SharePoint (Online) account.	`string` OAuth2 series required	Yes

Configuration	Description	Type	Required
`domain`	The domain of your SharePoint (Online) account.	`string`	Yes
`siteUrls`	The host URLs of your SharePoint (Online) account.	`array (string)` Specify the URL in the pattern `https://*`	Yes
`repositoryAdditionalProperties`	Additional properties to connect with your repository endpoint.	`object` This property has the following sub-properties. • `version` • `authType` • `s3bucketName` • `s3certificateName`	Yes
`s3bucketName`	The name of the Amazon S3 bucket that stores your Azure AD self-signed X.509 certificate.	`string` Azure AD App-Only auth required	No
`s3certificateName`	The name of the SSL certificate stored in your Amazon S3 bucket.	`string` Azure AD App-Only auth required	No

Configuration	Description	Type	Required
`authType`	The type of authentication you are using: `OAuth2`, `OAuth2Certificate` , `OAuth2App` , or `Basic`.	`string`	Yes
`version`	The SharePoint version you are using: `Online`.	`string (Online)` Azure AD App-Only auth required	Yes
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties. • `event` • `page` • `file` • `link` • `attachment` • `comment`	Yes

Configuration	Description	Type	Required
• event • page • file • link • attachment • comment	A list of objects that map the attributes or field names of your SharePoint (Online) pages and assets to Amazon Q index field names.	object These properties have the following sub-properties. • indexFieldName • indexFieldType • dataSourceFieldName • dateFieldFormat	No
indexFieldName	The field name of your SharePoint (Online) events, pages, files, links, attachments, or comments.	string	Yes
indexFieldType	The field type of your SharePoint (Online) events, pages, files, links, attachments, or comments.	string The allowed values are STRING, STRING_LIST , and DATE.	Yes
dataSourceFieldName	The data source field name of your SharePoint (Online) events, pages, files, links, attachments, or comments.	string	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The date format of your SharePoint (Online) events, pages, files, links, attachments, or comments.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties: • crawlAcl • crawlFiles • crawlPages • crawlEvents • crawlComments • crawlLinks • crawlAttachments • crawlListData • isCrawlLocalGroupMapping • maxFileSizeInMegaBytes • eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath	Yes

Configuration	Description	Type	Required
		• inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotePageNamePatterns	

Configuration	Description	Type	Required
• eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePa	A list of regular expression patterns to include/exclude specific files in your SharePoint (Online) data source. Files that match the patterns are included in the index. File that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.	array (string)	No

Configuration	Description	Type	Required
geNamePat terns • exclusion OneNotePa geNamePat terns			

Configuration	Description	Type	Required
• `crawlFiles` • `crawlPages` • `crawlEvents` • `crawlComments` • `crawlLinks` • `crawlAttachments` • `crawlListData` • `crawlAcl` **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.	Input TRUE to index.	`boolean`	No

Configuration	Description	Type	Required
• `isCrawlLocalGroupMapping` • `isCrawlAdGroupMapping`			
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string`	No
`type`	We recommend that you use `SHAREPOINTV2` as your data source type	`string` Valid values are `SHAREPOINTV2` and `SHAREPOINT` .	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information,	`boolean`	Yes

Configuration	Description	Type	Required
	see Identity crawler.		
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index	Yes

Configuration	Description	Type	Required

`secretARN`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your SharePoint. If you use basic authentic ation, provide the username and password. If you use OAuth 2.0 authentic ation, provide the username, password, client ID, and client secret.	`string`
		
		The minimum length is 20 and the maximum length is 2,048 characters.
		If you use basic authentication (`authType` should be `Basic`), the secret must contain a JSON structure with the following keys:
		
		`{ "username": " SharePoint (Online) account user name", "password": " SharePoint (Online) password" }`
		
		If you use Azure AD App-only authentication (`authType` should be `0Auth2Cer tificate`), the secret must contain a JSON structure with the following keys:
		
		`{`
			Yes

Configuration	Description	Type	Required

		<pre>{
		  "clientId": "SharePoint (Online) client ID",
		  "privateKey": " SharePoint (Online) private key"
		}</pre>
		If you use OAuth2 authentication (authType should be 0Auth) or Sharepoint App-Only authentication (authType should be 0Auth2App) the secret must contain a JSON structure with the following keys:
		<pre>{
		  "clientId": "SharePoint (Online) client ID",
		  "clientSecret": "SharePoint (Online) client secret",
		  "userName": "SharePoint (Online) account user name",
		  "password": " SharePoin</pre>	

Configuration	Description	Type	Required
		`t (Online) password"` }	
`version`	The version of this template that's currently supported.	`string`	No

SharePoint (Online) JSON schema

The following is the SharePoint (Online) JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["SHAREPOINTV2", "SHAREPOINT"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
```

```
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            },
            "domain": {
              "type": "string"
            },
            "siteUrls": {
              "type": "array",
              "items": {
                "type": "string",
                "pattern": "https://.*"
              }
            },
            "repositoryAdditionalProperties": {
              "type": "object",
              "properties": {
                "s3bucketName": {
                  "type": "string"
                },
                "s3certificateName": {
                  "type": "string"
                },
                "authType": {
                  "type": "string",
                  "enum": [
                    "OAuth2",
                    "OAuth2Certificate",
                    "OAuth2App",
                    "Basic"
                  ]
                },
                "version": {
                  "type": "string",
                  "enum": ["Online"]
                },
```

```
              "enableDeletionProtection": {
                "anyOf": [
                  {
                    "type": "boolean"
                  },
                  {
                    "type": "string",
                    "enum": ["true", "false"]
                  }
                ],
                "default": false
              },
              "deletionProtectionThreshold": {
                "type": "string",
                "default": "15"
              }
            },
            "required": ["authType", "version"]
          }
        },
        "required": ["siteUrls", "domain", "repositoryAdditionalProperties"]
      }
    },
    "required": ["repositoryEndpointMetadata"]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "event": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
```

```
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "page": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
```

```
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "file": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
```

```
        },
        "link": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "attachment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
```

```
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "comment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
```

```
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "eventTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "pageTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "linkTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionFilePath": {
        "type": "array",
        "items": {
```

```
            "type": "string"
          }
        },
        "exclusionFilePath": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionOneNoteSectionNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionOneNoteSectionNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
```

```
        },
        "inclusionOneNotePageNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionOneNotePageNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "crawlFiles": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlPages": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlEvents": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
```

```
          ]
        },
        "crawlComments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlLinks": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAttachments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlListData": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
```

```
          ]
        },
        "crawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlLocalGroupMapping": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlAdGroupMapping": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
```

```
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "type",
    "syncMode",
    "secretArn",
    "enableIdentityCrawler",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

SharePoint (Online) JSON schema example

The following is the SharePoint (Online) JSON schema example:

```
{
  "type": "SHAREPOINTV2",
  "syncMode": "FULL_CRAWL",
  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-sharepoint-
secret",
  "enableIdentityCrawler": "true",
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "tenantId": "1234567a-890b-1234-567c-123456789012",
      "domain": "example.sharepoint.com",
      "siteUrls": ["https://example.sharepoint.com/sites/mysite"],
      "repositoryAdditionalProperties": {
        "s3bucketName": "my-bucket",
        "s3certificateName": "my-certificate",
        "authType": "OAuth2",
        "version": "Online",
        "enableDeletionProtection": "false",
        "deletionProtectionThreshold": "15"
      }
    }
  },
  "repositoryConfigurations": {
    "event": {
```

```
      "fieldMappings": [
        {
          "indexFieldName": "event_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "page": {
      "fieldMappings": [
        {
          "indexFieldName": "page_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    }
  },
  "additionalProperties": {
    "eventTitleFilterRegEx": ["^.*$"],
    "pageTitleFilterRegEx": ["^.*$"],
    "linkTitleFilterRegEx": ["^.*$"],
    "inclusionFilePath": ["documents/"],
    "exclusionFilePath": ["drafts/"],
    "inclusionFileTypePatterns": ["*.docx"],
    "exclusionFileTypePatterns": ["*.tmp"],
    "inclusionFileNamePatterns": ["*report*"],
    "exclusionFileNamePatterns": ["*draft*"],
    "enableDeletionProtection": "false",
    "maxFileSizeInMegaBytes": "50"
  }
}
```

Connecting Amazon Q Business to SharePoint (Online) using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- SharePoint (Online) configuration properties
- SharePoint (Online) JSON schema for using the configuration property with AWS CloudFormation
- SharePoint (Online) YAML schema for using the configuration property with AWS CloudFormation

SharePoint (Online) configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-properties. • `siteUrls` • `domain` • `repositoryAdditionalProperties` • `tenantId`	Yes

Configuration	Description	Type	Required
`tenantId`	The tenant id of your SharePoint (Online) account.	`string` OAuth2 series required	Yes
`domain`	The domain of your SharePoint (Online) account.	`string`	Yes
`siteUrls`	The host URLs of your SharePoint (Online) account.	`array (string)` Specify the URL in the pattern `https://*`	Yes
`repositoryAdditionalProperties`	Additional properties to connect with your repository endpoint.	`object` This property has the following sub-properties. • `version` • `authType` • `s3bucketName` • `s3certificateName`	Yes
`s3bucketName`	The name of the Amazon S3 bucket that stores your Azure AD self-signed X.509 certificate.	`string` Azure AD App-Only auth required	No

Configuration	Description	Type	Required
`s3certificateName`	The name of the SSL certificate stored in your Amazon S3 bucket.	`string` Azure AD App-Only auth required	No
`authType`	The type of authentication you are using: `OAuth2`, `OAuth2Certificate` , `OAuth2App` , or `Basic`.	`string`	Yes
`version`	The SharePoint version you are using: `Online`.	`string (Online)` Azure AD App-Only auth required	Yes
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties. • `event` • `page` • `file` • `link` • `attachment` • `comment`	Yes

Configuration	Description	Type	Required
• event • page • file • link • attachment • comment	A list of objects that map the attributes or field names of your SharePoint (Online) pages and assets to Amazon Q index field names.	object These properties have the following sub-properties. • indexFieldName • indexFieldType • dataSourceFieldName • dateFieldFormat	No
indexFieldName	The field name of your SharePoint (Online) events, pages, files, links, attachments, or comments.	string	Yes
indexFieldType	The field type of your SharePoint (Online) events, pages, files, links, attachments, or comments.	string The allowed values are STRING, STRING_LIST , and DATE.	Yes
dataSourceFieldName	The data source field name of your SharePoint (Online) events, pages, files, links, attachments, or comments.	string	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The date format of your SharePoint (Online) events, pages, files, links, attachments, or comments.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties: • crawlAcl • crawlFiles • crawlPages • crawlEvents • crawlComments • crawlLinks • crawlAttachments • crawlListData • isCrawlLocalGroupMapping • maxFileSizeInMegaBytes • eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath	Yes

Configuration	Description	Type	Required
		• inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotePageNamePatterns	

Configuration	Description	Type	Required
• eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePa	A list of regular expression patterns to include/exclude specific files in your SharePoint (Online) data source. Files that match the patterns are included in the index. File that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.	array (string)	No

Configuration	Description	Type	Required
geNamePat terns • exclusion OneNotePa geNamePat terns			

Configuration	Description	Type	Required
• `crawlFiles` • `crawlPages` • `crawlEvents` • `crawlComments` • `crawlLinks` • `crawlAttachments` • `crawlListData` • `crawlAcl` **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.	Input TRUE to index.	`boolean`	No

Configuration	Description	Type	Required
• `isCrawlLocalGroupMapping` • `isCrawlAdGroupMapping`			
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string`	No
`type`	We recommend that you use `SHAREPOINTV2` as your data source type	`string` Valid values are `SHAREPOINTV2` and `SHAREPOINT` .	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information,	`boolean`	Yes

Configuration	Description	Type	Required
	see Identity crawler.		
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index	Yes

Configuration	Description	Type	Required

`secretARN`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your SharePoint. If you use basic authentic ation, provide the username and password. If you use OAuth 2.0 authentic ation, provide the username, password, client ID, and client secret.	`string`
		
		The minimum length is 20 and the maximum length is 2,048 characters.
		If you use basic authentication (`authType` should be `Basic`), the secret must contain a JSON structure with the following keys:
		
		`{ "username": " SharePoint (Online) account user name", "password": " SharePoint (Online) password" }`
		
		If you use Azure AD App-only authentication (`authType` should be `0Auth2Cer tificate`), the secret must contain a JSON structure with the following keys:
		
		`{`
			Yes

Configuration	Description	Type	Required

		<pre>{
		  "clientId": "SharePoint (Online) client ID",
		  "privateKey": " SharePoint (Online) private key"
		}</pre>
		If you use OAuth2 authentication (authType should be 0Auth) or Sharepoint App-Only authentication (authType should be 0Auth2App) the secret must contain a JSON structure with the following keys:
		<pre>{
		  "clientId": "SharePoint (Online) client ID",
		  "clientSecret": "SharePoint (Online) client secret",
		  "userName": "SharePoint (Online) account user name",
		  "password": " SharePoin</pre>	

Configuration	Description	Type	Required
		t (Online) *password*" }	
`version`	The version of this template that's currently supported.	`string`	No

SharePoint (Online) JSON schema for using the configuration property with AWS CloudFormation

The following is the SharePoint (Online) JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- SharePoint (Online) JSON schema for using the configuration property with AWS CloudFormation
- SharePoint (Online) JSON schema example for using the configuration property with AWS CloudFormation

SharePoint (Online) JSON schema for using the configuration property with AWS CloudFormation

The following is the SharePoint (Online) JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["SHAREPOINTV2", "SHAREPOINT"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
```

```
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            },
            "domain": {
              "type": "string"
            },
            "siteUrls": {
              "type": "array",
              "items": {
                "type": "string",
                "pattern": "https://.*"
              }
            },
            "repositoryAdditionalProperties": {
              "type": "object",
              "properties": {
                "s3bucketName": {
                  "type": "string"
```

```
            },
            "s3certificateName": {
              "type": "string"
            },
            "authType": {
              "type": "string",
              "enum": [
                "OAuth2",
                "OAuth2Certificate",
                "OAuth2App",
                "OAuth2_RefreshToken",
                "Basic"
              ]
            },
            "version": {
              "type": "string",
              "enum": ["Online"]
            },
            "enableDeletionProtection": {
              "anyOf": [
                {
                  "type": "boolean"
                },
                {
                  "type": "string",
                  "enum": ["true", "false"]
                }
              ],
              "default": false
            },
            "deletionProtectionThreshold": {
              "type": "string",
              "default": "15"
            }
          },
          "required": ["authType", "version"]
        }
      },
      "required": ["siteUrls", "domain", "repositoryAdditionalProperties"]
    }
  },
  "required": ["repositoryEndpointMetadata"]
},
"repositoryConfigurations": {
```

```
      "type": "object",
      "properties": {
        "event": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "page": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
```

```
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "file": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE", "LONG"]
                  },
```

```
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "link": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
```

```
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "attachment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
```

```
        },
        "comment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        }
      }
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "eventTitleFilterRegEx": {
          "type": "array",
          "items": {
```

```
            "type": "string"
          }
        },
        "pageTitleFilterRegEx": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "linkTitleFilterRegEx": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFilePath": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFilePath": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
```

```
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionOneNoteSectionNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionOneNoteSectionNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionOneNotePageNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionOneNotePageNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "crawlFiles": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlPages": {
          "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlEvents": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlComments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlLinks": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAttachments": {
          "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlListData": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "aclConfiguration": {
          "type": "string",
          "enum": [
            "ACLWithLDAPEmailFmt",
            "ACLWithManualEmailFmt",
            "ACLWithUsernameFmt"
          ]
        },
        "emailDomain": {
          "type": "string"
        },
        "isCrawlLocalGroupMapping": {
          "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlAdGroupMapping": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "type",
    "syncMode",
    "secretArn",
    "enableIdentityCrawler",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
```

```
}
```

SharePoint (Online) JSON schema example for using the configuration property with AWS CloudFormation

The following is the SharePoint (Online) JSON schema example for the configuration property for CloudFormation

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation SHAREPOINT Data Source Template",
  "Resources": {
    "DataSourceSharePoint": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MySharePointDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "SHAREPOINTV2",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-
sharepoint-secret",
          "enableIdentityCrawler": "true",
          "connectionConfiguration": {
            "repositoryEndpointMetadata": {
              "tenantId": "1234567a-890b-1234-567c-123456789012",
              "domain": "example.sharepoint.com",
              "siteUrls": ["https://example.sharepoint.com/sites/mysite"],
              "repositoryAdditionalProperties": {
                "s3bucketName": "my-bucket",
                "s3certificateName": "my-certificate",
                "authType": "OAuth2",
                "version": "Online",
                "enableDeletionProtection": "false",
                "deletionProtectionThreshold": "15"
              }
            }
          },
          "repositoryConfigurations": {
            "event": {
              "fieldMappings": [
```

```
                {
                  "indexFieldName": "event_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
            },
            "page": {
              "fieldMappings": [
                {
                  "indexFieldName": "page_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
            }
          },
          "additionalProperties": {
            "eventTitleFilterRegEx": ["^.*$"],
            "pageTitleFilterRegEx": ["^.*$"],
            "linkTitleFilterRegEx": ["^.*$"],
            "inclusionFilePath": ["documents/"],
            "exclusionFilePath": ["drafts/"],
            "inclusionFileTypePatterns": ["\\.docx"],
            "exclusionFileTypePatterns": ["\\.tmp"],
            "inclusionFileNamePatterns": ["*report*"],
            "exclusionFileNamePatterns": ["*draft*"],
            "enableDeletionProtection": "false",
            "maxFileSizeInMegaBytes": "50"
          }
        }
      }
    }
  }
}
```

SharePoint (Online) YAML schema for using the configuration property with AWS CloudFormation

The following is the SharePoint (Online) YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- SharePoint (Online) YAML schema for using the configuration property with AWS CloudFormation
- SharePoint (Online) YAML schema example for using the configuration property with AWS CloudFormation

SharePoint (Online) YAML schema for using the configuration property with AWS CloudFormation

The following is the SharePoint (Online) YAML schema for the configuration property for CloudFormation.

```
$schema: http://json-schema.org/draft-04/schema#
type: object
properties:
  type:
    type: string
    enum:
      - SHAREPOINTV2
      - SHAREPOINT
  syncMode:
    type: string
    enum:
      - FULL_CRAWL
      - FORCED_FULL_CRAWL
      - CHANGE_LOG
  secretArn:
    type: string
    minLength: 20
    maxLength: 2048
  enableIdentityCrawler:
    anyOf:
      - type: boolean
      - type: string
        enum:
          - true
          - false
  connectionConfiguration:
    type: object
    properties:
      repositoryEndpointMetadata:
```

```
        type: object
        properties:
          tenantId:
            type: string
            pattern: "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$"
            minLength: 36
            maxLength: 36
          domain:
            type: string
          siteUrls:
            type: array
            items:
              type: string
              pattern: "https://.*"
          repositoryAdditionalProperties:
            type: object
            properties:
              s3bucketName:
                type: string
              s3certificateName:
                type: string
              authType:
                type: string
                enum:
                  - OAuth2
                  - OAuth2Certificate
                  - OAuth2App
                  - OAuth2_RefreshToken
                  - Basic
              version:
                type: string
                enum:
                  - Online
              enableDeletionProtection:
                anyOf:
                  - type: boolean
                  - type: string
                    enum:
                      - true
                      - false
                default: false
              deletionProtectionThreshold:
                type: string
                default: "15"
```

```
            required:
              - authType
              - version
        required:
          - siteUrls
          - domain
          - repositoryAdditionalProperties
    required:
      - repositoryEndpointMetadata
  repositoryConfigurations:
    type: object
    properties:
      event:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      page:
        type: object
        properties:
          fieldMappings:
            type: array
```

```
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - DATE
                    - LONG
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      file:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - DATE
                    - LONG
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
```

```
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
        required:
          - fieldMappings
      link:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      attachment:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
```

```
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    comment:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
        required:
          - fieldMappings
  required: []
additionalProperties:
```

```
    type: object
    properties:
      eventTitleFilterRegEx:
        type: array
        items:
          type: string
      pageTitleFilterRegEx:
        type: array
        items:
          type: string
      linkTitleFilterRegEx:
        type: array
        items:
          type: string
      inclusionFilePath:
        type: array
        items:
          type: string
      exclusionFilePath:
        type: array
        items:
          type: string
      inclusionFileTypePatterns:
        type: array
        items:
          type: string
      exclusionFileTypePatterns:
        type: array
        items:
          type: string
      inclusionFileNamePatterns:
        type: array
        items:
          type: string
      exclusionFileNamePatterns:
        type: array
        items:
          type: string
      inclusionOneNoteSectionNamePatterns:
        type: array
        items:
          type: string
      exclusionOneNoteSectionNamePatterns:
        type: array
```

```
        items:
          type: string
      inclusionOneNotePageNamePatterns:
        type: array
        items:
          type: string
      exclusionOneNotePageNamePatterns:
        type: array
        items:
          type: string
      crawlFiles:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlPages:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlEvents:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlComments:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlLinks:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
```

```
            - false
      crawlAttachments:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlListData:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlAcl:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      aclConfiguration:
        type: string
        enum:
          - ACLWithLDAPEmailFmt
          - ACLWithManualEmailFmt
          - ACLWithUsernameFmt
      emailDomain:
        type: string
      isCrawlLocalGroupMapping:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      isCrawlAdGroupMapping:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
```

```
      maxFileSizeInMegaBytes:
        type: string
    required: []
  version:
    type: string
    anyOf:
      - pattern: 1.0.0
required:
  - type
  - syncMode
  - secretArn
  - enableIdentityCrawler
  - connectionConfiguration
  - repositoryConfigurations
  - additionalProperties
```

SharePoint (Online) YAML schema example for using the configuration property with AWS CloudFormation

The following is the SharePoint (Online) YAML example for the Configuration property for CloudFormation:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: CloudFormation SHAREPOINT Data Source Template
Resources:
  DataSourceSharePoint:
    Type: AWS::QBusiness::DataSource
    Properties:
      ApplicationId: app12345-1234-1234-1234-123456789012
      IndexId: indx1234-1234-1234-1234-123456789012
      DisplayName: MySharePointDataSource
      RoleArn: arn:aws:iam::123456789012:role/qbusiness-data-source-role
      Configuration:
        type: SHAREPOINTV2
        syncMode: FULL_CRAWL
        secretArn: arn:aws:secretsmanager:us-west-2:123456789012:secret:my-sharepoint-
secret
        enableIdentityCrawler: "true"
        connectionConfiguration:
          repositoryEndpointMetadata:
            tenantId: 1234567a-890b-1234-567c-123456789012
            domain: example.sharepoint.com
            siteUrls:
```

```
        - https://example.sharepoint.com/sites/mysite
      repositoryAdditionalProperties:
        s3bucketName: my-bucket
        s3certificateName: my-certificate
        authType: OAuth2
        version: Online
        enableDeletionProtection: "false"
        deletionProtectionThreshold: "15"
    repositoryConfigurations:
      event:
        fieldMappings:
          - indexFieldName: event_id
            indexFieldType: STRING
            dataSourceFieldName: id
            dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
      page:
        fieldMappings:
          - indexFieldName: page_id
            indexFieldType: STRING
            dataSourceFieldName: id
            dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
    additionalProperties:
      eventTitleFilterRegEx:
        - "^.*$"
      pageTitleFilterRegEx:
        - "^.*$"
      linkTitleFilterRegEx:
        - "^.*$"
      inclusionFilePath:
        - documents/
      exclusionFilePath:
        - drafts/
      inclusionFileTypePatterns:
        - ".docx"
      exclusionFileTypePatterns:
        - ".tmp"
      inclusionFileNamePatterns:
        - "*report*"
      exclusionFileNamePatterns:
        - "*draft*"
      enableDeletionProtection: "false"
      maxFileSizeInMegaBytes: "50"
```

How Amazon Q Business connector crawls SharePoint (Online) ACLs

When you connect an SharePoint (Online) data source to Amazon Q Business, Amazon Q crawls ACL information attached to a document (user and group information) from your SharePoint (Online) instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

To filter using a username, use the **User principal name** from your Azure portal. For example, johnstiles@amazonq.onmicrosoft.com.

When you use a SharePoint group for user context filtering, calculate the group ID as follows:

For local groups

1. Get the site name. For example, `https://host.onmicrosoft.com/sites/siteName`.
2. Take the SHA256 hash of the site name. For example, `430a6b90503eef95c89295c8999c7981`.
3. Create the group ID by concatenating the SHA256 hash with a vertical bar (|) and the group name. For example, if the group name is "local group name", the group ID is the following:

   `"430a6b90503eef95c89295c8999c7981 | localGroupName"` (with a space before and after the vertical bar).

For Microsoft Entra ID (formerly Azure AD) groups

1. You must integrate the Microsoft Entra ID (formerly Azure AD) with Amazon Identity Center and use the same group name present on Azure portal.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

SharePoint (Online) data source connector field mappings

To help you structure data for retrieval and chat filtering, Amazon Q Business crawls data source document attributes or metadata and maps them to fields in your Amazon Q index.

Amazon Q has reserved fields that it uses when querying your application. When possible, Amazon Q automatically maps these built-in fields to attributes in your data source. If a built-in field doesn't have a default mapping, or if you want to map additional index fields, use the custom field mappings to specify how a data source attribute maps to your Amazon Q application. You create field mappings by editing your data source after your application environment and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Sharepoint connector supports the following entities and the associated reserved and custom attributes.

> **Important**
>
> If you map any SharePoint (Online) field to Amazon Q document title and document body fields, Amazon Q will generate responses from data in the document title and body.

> **Note**
>
> You can map any Sharepoint field to the document title or document body Amazon Q reserved/default index fields.

Supported entities and field mappings

- Files
- Events
- Pages
- Links
- Attachments

- Comments

Files

Sharepoint field name	Index field name	Description	Data type
title	sp_title	Custom	String
sourceUri	_source_uri	Default	String
checkInComment	sp_checkInComment	Custom	String
size	sp_sizeLong	Custom	Long (numeric)
lastModifiedDateTime	_last_updated_at	Default	Date
createdAt	_created_at	Default	Date
author	_authors	Default	String list
majorVersion	sp_majorVersion	Custom	String
uiVersionLabel	sp_uiVersionLabel	Custom	String
uniqueId	sp_uniqueId	Custom	String
irmEnabled	sp_irmEnabled	Custom	String
checkOutType	sp_checkOutType	Custom	String
category	_category	Default	String
modifiedBy	sp_modifiedBy	Custom	String
level	sp_level	Custom	String
uiVersion	sp_uiVersion	Custom	String
contentTag	sp_contentTag	Custom	String

Sharepoint field name	Index field name	Description	Data type
eTag	sp_eTag	Custom	String
oneNoteDocument	sp_oneNoteDocument	Custom	String
oneNoteSection	sp_oneNoteSection	Custom	String
oneNotePage	sp_oneNotePage	Custom	String

Events

Sharepoint field name	Index field name	Description	Data type
title	sp_title	Custom	String
lastModifiedDateTime	_last_updated_at	Default	Date
sourceUri	_source_uri	Default	String
attachments	sp_hasAttachments	Custom	String
createdDate	_created_at	Default	Date
authorId	sp_authorId	Custom	String
editorId	sp_editorId	Custom	String
location	sp_location	Custom	String
eventDate	sp_eventDate	Custom	Date
eventEndDate	sp_eventEndDate	Custom	Date
ifRecurrence	sp_ifRecurrence	Custom	String

Sharepoint field name	Index field name	Description	Data type
ifAllDayEvent	sp_ifAllDayEvent	Custom	String
category	_category	Default	String
eventCategory	sp_eventcategory	Custom	String

Pages

Sharepoint field name	Index field name	Description	Data type
createdDateTime	_created_at	Default	Date
lastModifiedDateTime	_last_updated_at	Default	Date
title	sp_title	Custom	String
sourceUri	_source_uri	Default	String
firstPublishedDate	sp_firstPublishedDate	Custom	Date
authorId	sp_authorId	Custom	String
editorId	sp_editorId	Custom	String
category	_category	Default	String

Links

Sharepoint field name	Index field name	Description	Data type
createdAt	_created_at	Default	Date

Sharepoint field name	Index field name	Description	Data type
lastModifiedDateTime	_last_updated_at	Default	Date
title	sp_title	Custom	String
sourceUri	_source_uri	Default	String
fileType	sp_fileType	Custom	String
fileDirPath	sp_fileDirPath	Custom	String
firstPublishedDate	sp_firstPublishedDate	Custom	Date
authorId	sp_authorId	Custom	String
editorId	sp_editorId	Custom	String
category	_category	Default	String
size	sp_sizeLong	Custom	Long (numeric)

Attachments

Sharepoint field name	Index field name	Description	Data type
title	sp__title	Custom	String
parentCreatedDate	_created_at	Default	Date
sourceUri	_source_uri	Default	String
parentModifiedDate	_last_updated_at	Custom	Date
parentListId	sp_parentListId	Custom	String
parentTitle	sp_parentTitle	Custom	String

Sharepoint field name	Index field name	Description	Data type
category	_category	Default	String

Comments

Sharepoint field name	Index field name	Description	Data type
createdDateTime	_created_at	Default	Date
likedBy	sp_likedBy	Custom	String
sourceUri	_source_uri	Custom	String
isReply	sp_isReply	Custom	String
author	_authors	Default	String list
listId	sp_listId	Custom	String
category	_category	Default	String
replyCount	sp_replyCount	Custom	String
parentTitle	sp_parentTitle	Custom	String

IAM role for SharePoint (Online) connector

> **Note**
>
> **(Optional)** If you use **Azure App-Only authentication**, you also need to add permissions for Amazon Q to access the certificate stored in your Amazon S3 bucket.

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
```

```
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    }
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

To ensure that Amazon Q Business is able to access Amazon S3 you objects:

If you are using Microsoft Entra ID (formerly Azure AD) App only authentication, you must ensure that Amazon Q Business is able access Amazon S3 to get the objects in your bucket. The following policy statement is provides permissions to access Amazon S3:

```
    {
    "Version": "2012-10-17",       ,
    "Statement": [
    {
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        }
        ]
     }
```

If using a VPC:

If you are using a VPC, you must ensure that the permissions included in the following policy statement are included in your policy statement:

```
    {
    "Version": "2012-10-17",       ,
    "Statement": [
     {
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
```

```
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
"qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
"qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
        ]
    }
```

Understand error codes in the SharePoint (Online) connector

The following table provides information about error codes you may see for the Microsoft SharePoint connector and suggested resolutions. If you used the Amazon Q section of the AWS console to configure your connectors, be sure to make the changes associated with an error through the console as well. You can refer to the Microsoft SharePoint documentation for more information regarding SharePoint settings and details.

Authentication issues

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5001	Authentication failed. Configuration might contain wrong credentials.	Provide valid credentials like username, password or client Id, client secret and tenant Id.	Occurs during initial connector setup or when authentication credentials expire	Console: During configuration or Sync run history
SPE-5124	There was a problem while retrieving authType. Auth-Type	Ensure AUTH Type in configuration must be not null.	Authentication type configuration error	Console: Configuration page

Error code	Error message	Suggested resolution	Context	Where to find error
	might be empty or null.			
SPE-5129	There was a problem while retrieving password. Password might be empty or null.	Provide password.	Basic authentic ation configuration error	Console: During initial setup
SPE-5130	There was a problem while retrieving username. Username might be empty or null.	Provide username.	Basic authentic ation configuration error	Console: During initial setup
SPE-5136	The provided authType was not a valid Sharepoint Connector authentic ation method.	Provide valid authType. The value of authType should be one of [Basic, OAuth2Cer tificate, OAuth2].	Authentication method configura tion error	Console: Configura tion page

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5125	There was a problem while retrievin g clientId. Client ID might be empty or null.	Provide Client Id.	OAuth configura tion error	Console: Authentic ation Configuration
SPE-5126	There was a problem while retrieving clientSec ret. Client Secret might be empty or null.	Provide Client Secret.	OAuth configura tion error	Console: Authentic ation Configuration
SPE-5127	There was a problem while retrieving tenantId. Tenant ID might be empty or null.	Provide Tenant Id.	SharePoint tenant configuration error	Console: Authentic ation Configuration

SharePoint Configuration issues

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5135	The provided version was not a valid Sharepoint Connector version. Version should be one of [Online, Server].	Version should be one of [Online, Server].	SharePoint version selection error	Console: During initial setup
SPE-5138	There was a problem while retrieving onPremVersion. On prem Version might be empty or null	Ensure onPremVersion is not be null or non-empty.	SharePoint on-premises version error	Console: Version Configuration
SPE-5139	The provided onPremVersion was not valid Sharepoint on-prem version. On prem	Provide a valid onPremVersion. On prem version should be one of [2013, 2016, 2019, SubscriptionEdition].	SharePoint on-premises version selection error	Console: Version Configuration

Error code	Error message	Suggested resolution	Context	Where to find error
	version should be one of [2013, 2016, 2019, SubscriptionEdition].			
SPE-5121	There was a problem while retrieving values for crawl entities. Values might be empty or incorrect. It should be either true or false.	In the connector's settings, ensure all crawl options are set to either 'true' or 'false'. These settings determine what content types are indexed.	Crawler configuration error	Console: Crawl Configuration
SPE-5122	There was a problem while retrieving domain. Domain might be empty or null.	Provide a valid SharePoint domain name in the connector configuration.	Domain configuration error during SharePoint connection setup.	Console: Domain Configuration

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5123	There was a problem while retrievin g version. Version might be empty or null.	Provide valid version and it should not be null.	SharePoint version configuration error	Console: Version Configuration

Network and Connectivity issues

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5004	Inet Address validation Failed.	Check your network configuration and ensure the SharePoint server address is accessibl e from your network. Verify DNS resolution and network routing are properly configure d.	Network address validation error	CloudWatch Logs during sync
SPE-5005	Failed : HTTP protocol violation has occurred.	Try running the connector again.	Occurs when the connector is configured to use a proxy but cannot establish connectio n.	CloudWatch Logs during sync

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5200	There was a problem while connecting to the URL.	Verify that the SharePoint site URL is accessible and that you have proper network connectivity. Check SharePoint site status and your network configura tion.	Site connectivity error	Console: Sync run history
SPE-5002	SPE-5002 Connectio n failed due to wrong credentia ls or invalid sites. Update your configura tion and try again.	Provide valid Host URL or Domain.	Happens during connector configura tion when trying to establish initial connection	Console: Basic Configuration
SPE-5003	Provided URL is incorrect	Provide correct URL.	Generic URL validation error	Console: Site Configuration

LDAP Configuration issues

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5009	There was a problem while connecting to LDAP. Check LDAP configuration.	Provide valid LDAP configuration details.	LDAP connection failure	Console: LDAP Configuration
SPE-5140	There was a problem while retrieving ldapUrl. LDAP Url might be empty or null.	Ensure ldapUrl is not null or empty.	LDAP configuration error	Console: LDAP Configuration
SPE-5141	There was a problem while retrieving baseDn. Base DN might be empty or null.	Ensure baseDn is not be null or empty.	LDAP configuration error	Console: LDAP Configuration
SPE-5146	There was a problem while retrieving ldapUsern	Ensure ldapUser is not null or empty.	LDAP authentication error	Console: LDAP Configuration

Error code	Error message	Suggested resolution	Context	Where to find error
	ame. LDAP Username might be empty or null.			
SPE-5147	There was a problem while retrieving ldapPassword. LDAP Password might be empty or null.	Ensure ldapPassword is not null or empty.	LDAP authentication error	Console: LDAP Configuration

Microsoft Entra ID (formerly Azure AD) Configuration issues

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5152	There was a problem while retrieving AD Client ID. AD Client ID should not be empty.	Ensure AD Client Id must be non-empty.	Microsoft Entra ID (formerly Azure AD) configuration error	Console: Microsoft Entra ID (formerly Azure AD) Configuration

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5153	Invalid AD Client Id pattern.	Provide valid AD Client Id pattern.	Microsoft Entra ID (formerly Azure AD) Client ID format error	Console: Microsoft Entra ID (formerly Azure AD) Configuration
SPE-5154	There was a problem while retrieving AD Client Secret. AD Client Secret should not be empty.	Ensure AD Client Secret is non-empty.	Microsoft Entra ID (formerly Azure AD) configuration error	Console: Microsoft Entra ID (formerly Azure AD) Configuration

Document Access and Permissions issues

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5144	There was a problem while retrieving aclConfig uration. ACL Configura tion might be empty, null or invalid	Provide valid aclConfiguration. aclConfiguration should be one of [ACLWithLD APEmailFm t, ACLWithMa nualEmailFmt, ACLWithUs ernameFmt].	ACL configuration error	Console: Access Control Configura tion

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5145	There was a problem while retrieving emailDomain. Email Domain might be empty or null.	Ensure emailDomain is not null or empty.	Email domain configuration error	Console: Domain Configuration
SPE-5155	There can't be more than one site for SharePoint on-prem app-only authentication.	Ensure that their must be only single site present for SharePoint on-prem app-only authentication.	SharePoint on-premises app authentication configuration error	Console: Site Configuration

Security Configuration issues

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5008	Valid SSL Certificate could not be found for connector.	Upload a valid SSL certificate. For SharePoint on-premises installations, ensure you have exported your SharePoint	SSL certificate validation failure	Console: Security Configuration

Error code	Error message	Suggested resolution	Context	Where to find error
		SSL certificate and uploaded it to the connector.		

IAM Configuration issues

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5101	There was a problem while retrieving dataSourceIamRoleArn. Data Source IAM Role ARN might be empty or null.	Verify that the IAM role exists and has the correct permissions. Check the IAM console to ensure the role is properly configured.	This error occurs when the connector cannot access the required IAM role during synchronization.	Console: IAM Configuration

Site Configuration issues

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5128	There was a problem while retrieving siteUrls. Site URLs	Provide at least one Site Url.	Site configuration error	Console: Site Configuration

Error code	Error message	Suggested resolution	Context	Where to find error
	might be empty or null.			
SPE-5131	There was a problem while retrieving username. Email was invalid.	Provide valid email address.	User email validation error	Console: User Configuration
SPE-5132	There was a problem while retrievin g url. This URL was invalid.	Provide a valid URL.	Provide a valid SharePoint site URL in the format https://your-sharepoint-site.com	Console: Site Configuration
SPE-5149	The provided siteUrls contain duplicate sites. Remove duplicates.	Ensure SiteUrls must not be the same.	Duplicate site URL configuration error	Console: Site Configuration

Other Configuration issues

Error code	Error message	Suggested resolution	Context	Where to find error
SPE-5133	There was a problem while retrieving s3CertificateName. S3 Certificate Name might be empty or null.	When using certificate-based authentication, upload your authentication certificate to an S3 bucket and provide the certificate name and bucket details in the connector configuration.	S3 certificate configuration error	Console: Security Configuration
SPE-5134	There was a problem while retrieving s3BucketName. S3 Bucket Name might be empty or null	When using certificate-based authentication, upload your authentication certificate to an S3 bucket and provide the certificate name and bucket details in the connector configuration.	S3 bucket configuration error	Console: S3 Configuration
SPE-5151	Error parsing the field value. Size is over maximum allowed limit.	Reduce the field value size to within the maximum allowed limit.	Field size limit exceeded	Console: Field Configuration

Connecting SharePoint Server 2016 to Amazon Q Business

Microsoft SharePoint is a collaborative website building service that lets you customize web content and create web pages, web sites, document libraries, and lists. You can connect a SharePoint Server 2016 instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Amazon Q supports Microsoft SharePoint Server (2016, 2019, and Subscription Edition).

Topics

- Known limitations for the Amazon Q Business SharePoint Server 2016 connector
- SharePoint Server 2016 connector overview
- Prerequisites for connecting Amazon Q Business to SharePoint Server 2016
- Connecting Amazon Q Business to SharePoint Server 2016 using the console
- Connecting Amazon Q Business to SharePoint Server 2016 using APIs
- Connecting Amazon Q Business to SharePoint Server 2016 using AWS CloudFormation
- How Amazon Q Business connector crawls SharePoint Server 2016 ACLs
- Amazon Q Business SharePoint Server 2016 data source connector field mappings
- IAM role for Amazon Q Business SharePoint Server 2016 connector
- Understand error codes in the SharePoint Server 2016 connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Amazon Q Business SharePoint Server 2016 connector

The SharePoint Server 2016 connector has the following known limitations:

- The SharePoint Server connector supports custom field mappings only for the **Files** entity.

- For all SharePoint Server versions, the ACL token must be in lower case. For **Email with Domain from IDP** and **Email ID with Custom Domain** ACL, for example: *user@sharepoint2019.com*. For **Domain\User with Domain** ACL, for example: *sharepoint2013\user*.
- If an entity name has a % character in its name, the connector will skip these files due to API limitations.
- OneNote can only be crawled by the connector using a Tenant ID, and with OAuth 2.0, OAuth 2.0 refresh token, or SharePoint App Only authentication activated for SharePoint Online.
- The connector crawls the first section of a OneNote document using its default name only, even if the document is renamed.
- The connector crawls links in SharePoint 2016 if **Links** is selected as an entity to be crawled.
- The connector crawls only list attachments and comments when **List Data** is selected as an entity to be crawled.
- The connector crawls event attachments only when **Events** is also selected as an entity to be crawled.
- To crawl nested groups using **Identity crawler**, you have to activate Local as well as AD Group Crawling.
- To use **Identity Crawler** with SharePoint Server 2016 to crawl nested groups, you have to enable both Local and AD Group Crawling.
- Query responses based on AD Group ACLs are not supported for SharePoint Server 2016. You need to add users and groups directly to your document permissions list.
- When Access Control Lists (ACLs) are enabled, the "Sync only new or modified content" option is not available due to SharePoint Server 2016 API limitations. We recommend using "Full sync" or "New, modified, or deleted content sync" modes instead, or disable ACLs if you need to use this sync mode.

SharePoint Server 2016 connector overview

The following table gives an overview of the Amazon Q Business SharePoint Server 2016 connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	NTLM, Kerberos, SharePoint App-Only (Client Credentials Flow)

Category	Feature	Support
	Authentication credentials	**NTLM** • SharePoint admin username • SharePoint admin password If you're using **Email ID with Domain from IDP** to crawl ACLs, then you also need to add a: • LDAP Server Endpoint • LDAP Search Base • LDAP username • LDAP password **Kerberos** • SharePoint admin username • SharePoint admin password If you're using **Email ID with Domain from IDP** to crawl ACLs, then you also need to add a: • LDAP Server Endpoint • LDAP Search Base • LDAP username • LDAP password **SharePoint App-Only (Client Credentials Flow)** • Tenant ID • SharePoint App-Only client ID

Category	Feature	Support
		• SharePoint App-Only client secret If you're using **Email ID with Domain from IDP** to crawl ACLs, then you also need to add a: • LDAP Server Endpoint • LDAP Search Base • LDAP username • LDAP password
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Integration with Identity Provider (IdP)	Yes. LDAP.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	Yes. Supports custom metadata for **File** entity only.

Category	Feature	Support
	Entities	Yes. The following entities are supported: • Files • Attachments • Links • Lists • Pages • Events • Comments See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include/exclude by **Links** • Include/exclude by **Pages** • Include/exclude by **Events** • Include/exclude by file name • Include/exclude by file path • Include/exclude by file type • Include/exclude by **OneNote Section** name • Include/exclude by **OneNote Page** name
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to SharePoint Server 2016

The following page outlines the prerequisites you need to complete before connecting SharePoint Server 2016 to Amazon Q, based on the authentication mode of your choice.

Topics

- Prerequisites for using NTLM authentication
- Prerequisites for using Kerberos authentication
- Prerequisites for using SharePoint App-Only authentication

Prerequisites for using NTLM authentication

If you're using NTLM authentication, make sure you've completed the following steps in SharePoint:

- Copied your SharePoint instance URLs. The format for the host URL you enter is *`https://yourdomain.sharepoint.com/sites/mysite`*. Your URL must start with `https` and contain `sharepoint.com`.
- Copied the domain name of your SharePoint instance URL.
- Generated an SSL certificate and uploaded it to an Amazon S3 bucket.
- Noted the username and password that you use to connect to SharePoint.

(Optional) If you're using Email ID with Domain from IDP to control access to your documents, make sure you've completed the following steps:

- Copied your LDAP Server Endpoint (endpoint of LDAP server including protocol and port number). For example: *`ldap://example.com:389`*.
- Copied your LDAP Search Base (search base of the LDAP user). For example: *`CN=Users,DC=sharepoint,DC=com`*.
- Copied your LDAP username and LDAP password.

(Optional) If using Email ID with Custom Domain for access control, complete the following step:

- Noted your custom email domain value—for example: *`"amazon.com"`*.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your SharePoint Server 2016 authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Prerequisites for using Kerberos authentication

If you're using Kerberos authentication, make sure you've completed the following steps in SharePoint:

- Copied your SharePoint instance URLs. The format for the host URL you enter is *`https://yourdomain.sharepoint.com/sites/mysite`*. Your URL must start with `https` and contain `sharepoint.com`.
- Copied the domain name of your SharePoint instance URL.
- Generated an SSL certificate and uploaded it to an Amazon S3 bucket.
- Noted the username and password that you use to connect to SharePoint.

(Optional) If you're using Email ID with Domain from IDP to control access to your documents, make sure you've completed the following steps:

- Copied your LDAP Server Endpoint (endpoint of LDAP server including protocol and port number). For example: *`ldap://example.com:389`*.
- Copied your LDAP Search Base (search base of the LDAP user). For example: *`CN=Users,DC=sharepoint,DC=com`*.

- Copied your LDAP username and LDAP password.

(Optional) If using Email ID with Custom Domain for access control, complete the following step:

- Noted your custom email domain value—for example: *"amazon.com"*.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your SharePoint Server 2016 authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Prerequisites for using SharePoint App-Only authentication

If you're using SharePoint App-Only authentication, make sure you've completed the following steps in SharePoint:

- Copied the SharePoint client ID generated when you registered App Only at Site Level. ClientID format is ClientID@TenantId. For example, *ffa956f3-8f89-44e7-b0e4-49670756342c@888d0b57-69f1-4fb8-957f-e1f0bedf82fe*.
- Copied the SharePoint client secret generated when you registered App Only at Site Level.

> **Important**
>
> **Note:** Because client IDs and client secrets are generated for single sites only when you register SharePoint Server for App Only authentication, only one site URL is supported for SharePoint App Only authentication.

- Noted the Tenant ID of your SharePoint account.
- Noted your **LDAP Server Endpoint**, **LDAP Search Base**, **LDAP username**, and **LDAP password**.

> **Note**
>
> SharePoint App-Only Authentication is *not* supported for SharePoint 2013 version.

(Optional) If you're using Email ID with Domain from IDP to control access to your documents, make sure you've completed the following steps:

- Copied your LDAP Server Endpoint (endpoint of LDAP server including protocol and port number). For example: `ldap://example.com:389`.
- Copied your LDAP Search Base (search base of the LDAP user). For example: `CN=Users,DC=sharepoint,DC=com`.
- Copied your LDAP username and LDAP password.

(Optional) If using Email ID with Custom Domain for access control, complete the following step:

- Noted your custom email domain value—for example: `"amazon.com"`.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.

- Stored your SharePoint Server 2016 authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to SharePoint Server 2016 using the console

The following procedure outlines how to connect Amazon Q Business to SharePoint Server 2016 using the AWS Management Console.

Connecting Amazon Q to SharePoint Server 2016

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **SharePoint** data source to your Amazon Q application.
5. Then, on the **SharePoint Server 2016** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

   > **Note**
   >
   > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, enter the following information:

a. In **Source**, for **Hosting Method** – Choose **SharePoint Server**.

b. **Choose SharePoint Version** – Choose **SharePoint 2016**.

c. **Site URLs specific to your SharePoint repository** – Enter the SharePoint host URLs. The format for the host URLs you enter is *`https://yourcompany/sites/mysite`*. The URL must start with `https` protocol. Separate URLs with a new line. You can add up to 100 URLs.

d. **Domain** – Enter the SharePoint domain.

e. **SSL certificate location** – Enter the Amazon S3 path to your SSL certificate file.

8. For **Web proxy – *optional*** – Enter the host name (without the `http://` or `https://` protocol), and the port number used by the host URL transport protocol. The numeric value of the port number must be between 0 and 65535.

9. For **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. You can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details.See Authorization for more details. For SharePoint Server, you can choose from the following ACL options:

   a. **Email ID with Domain from IDP** – Access control is based on email IDs that are extracted from email domains fetched from the underlying identity provider (IdP). You provide the IdP connection details in your Secrets Manager secret during **Authentication**.

   b. **Email ID with Custom Domain** – Access control is based on email IDs. Provide the email domain value. For example, *`"amazon.com"`*. The email domain is used to construct the email ID for access control. You must enter your email domain using **Add Email Domain**.

   See Authorization for more details.

10. For **Authentication**, choose between **SharePoint App-Only authentication**, **NTLM authentication**, and **Kerberos authentication**, based on your use case.

    a. Enter the following information for both **NTLM authentication** and **Kerberos authentication**:

       For **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your SharePoint authentication credentials. If you choose to create a secret,

an AWS Secrets Manager secret window opens. Enter the following information in the window:

- **Secret name** – A name for your secret.
- **Username** – Username for your SharePoint account.
- **Password** – Password for your SharePoint account.

If using **Email ID with Domain from IDP**, also enter your:

- **LDAP Server Endpoint** – Endpoint of LDAP server, including protocol and port number. For example: *ldap://example.com:389*.
- **LDAP Search Base** – Search base of LDAP user. For example: *CN=Users,DC=sharepoint,DC=com*.
- **LDAP username** – Your LDAP username.
- **LDAP Password** – Your LDAP password.

b. Enter the following information for **SharePoint App-Only authentication**:

For **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your SharePoint authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens. Enter the following information in the window:

- **Secret name** – A name for your secret.
- **Client ID** – The SharePoint client ID that you generated when you registered App Only at Site Level. The ClientID format is ClientID@TenantId. For example, *ffa956f3-8f89-44e7-b0e4-49670756342c@888d0b57-69f1-4fb8-957f-e1f0bedf82fe*.
- **SharePoint client secret** – The SharePoint client secret generated when your register for App Only at Site Level.

  Note: Because client IDs and client secrets are generated for single sites only when you register SharePoint Server for App Only authentication, only one site URL is supported for SharePoint App Only authentication.

If using **Email ID with Domain from IDP**, also enter your:

- **LDAP Server Endpoint** – Endpoint of LDAP server, including protocol and port number. For example: *ldap://example.com:389*.
- **LDAP Search Base** – Search base of LDAP user. For example: *CN=Users,DC=sharepoint,DC=com*.
- **LDAP username** – Your LDAP user name.
- **LDAP Password** – Your LDAP password.

11. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

12. **Identity crawler** – Amazon Q crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. Only **Local Group Members** will be crawled by **Identity crawler**. For more information, see Identity crawler.

13. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.

14. In **Sync scope**, choose from the following options :

    a. **Select entities** – Choose the entities that you want to crawl. You can select to crawl **All** entities or any combination of **Files**, **Attachments**, **Links**, **Pages**, **Events** and **List Data**.

b. In **Additional configuration – *optional***, for **Entity regex patterns** – Add regular expression patterns for **Links**, **Pages**, and **Events** to include specific entities instead of syncing all your documents.

c. **Regex patterns** – Add regular expression patterns to include or exclude files by **File path**, **File name**, **File type**, **OneNote section name**, and **OneNote page name** instead of syncing all your documents. You can add up to 100 patterns.

> **Note**
>
> Any valid regex pattern is supported. For example, if you use the regex `^QBusiness*`, any content starting with the word `QBusiness` followed by any number of characters will be filtered (`QBusiness_doc1` or `QBusiness`, but not `doc1_QBusiness`).

d. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

To extract audio transcriptions and video content, enable processing for the following file types:

e. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

15. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

- **Full sync** – Sync all content regardless of the previous sync status.
- **New or modified content sync** – Sync only new and modified documents.
- **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

For more details, see Sync mode.

16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
18. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages,

including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to SharePoint Server 2016 using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- SharePoint Server 2016 configuration properties
- SharePoint Server 2016 JSON schema
- SharePoint Server 2016 JSON schema example

SharePoint Server 2016 configuration properties

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-properties.	Yes

Configuration	Description	Type	Required
		• siteUrls • domain • repository Additional Properties • tenantId	
tenantId	The tenant id of your SharePoint account.	string OAuth2 series required	Yes
domain	The domain of your SharePoint account.	string	Yes
siteUrls	The host URLs of your SharePoint account.	array (string) Specify the URL in the pattern https://*	Yes
repository Additional Properties	Additional properties to connect with your repository endpoint.	object This property has the following sub-properties. • version • authType • onPremVersion	Yes
authType	The type of authentication you are using: NTLM, Kerberos, or OAuth2App .	string	Yes

Configuration	Description	Type	Required
`version`	The SharePoint version you are using: `Sever`.	`string (Server)`	Yes
`onPremVersion`	The SharePoint version that you are using.	`string` Valid values are (empty), `2013`, `2016`, `2019`, and `SubscriptionEdition` .	Yes
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties. • `event` • `page` • `file` • `link` • `attachment` • `comment`	Yes

Configuration	Description	Type	Required
• event • page • file • link • attachment • comment	A list of objects that map the attributes or field names of your SharePoint Server 2016 pages and assets to Amazon Q index field names.	object These properties have the following sub-properties. • indexFieldName • indexFieldType • dataSourceFieldName • dateFieldFormat	No
indexFieldName	The field name of your SharePoint Server 2016 events, pages, files, links, attachments, or comments.	string	Yes
indexFieldType	The field type of your SharePoint Server 2016 events, pages, files, links, attachments, or comments.	string The allowed values are STRING, STRING_LIST , and DATE.	Yes
dataSourceFieldName	The data source field name of your SharePoint Server 2016 events, pages, files, links, attachments, or comments.	string	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The date format of your SharePoint Server 2016 events, pages, files, links, attachments, or comments.	`string` Specify the date format in the form `yyyy-MM-dd"T"HH:mm:ss"Z"`	No

Configuration	Description	Type	Required
`additionalProperties`	Additional configuration options for your content in your data source.	`object` This property has the following sub-properties: • `crawlAcl` • `crawlFiles` • `crawlPages` • `crawlEvents` • `crawlComments` • `crawlLinks` • `crawlAttachments` • `crawlListData` • `isCrawlLocalGroupMapping` • `isCrawlAdGroupMapping` • `aclConfiguration` • `emailDomain` • `maxFileSizeInMegaBytes` • `eventTitleFilterRegEx` • `pageTitleFilterRegEx` • `linkTitleFilterRegEx`	Yes

Configuration	Description	Type	Required
		• inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotePageNamePatterns	

Configuration	Description	Type	Required
		• `proxyHost` • `proxyPort`	

Configuration	Description	Type	Required
• eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePa	A list of regular expression patterns to include/exclude specific files in your SharePoint data source. Files that match the patterns are included in the index. File that don&t match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn&t included in the index.	array (string)	No

Configuration	Description	Type	Required
geNamePat terns • exclusion OneNotePa geNamePat terns • emailDomain			
aclConfig uration	Specifes how your ACL is configured.	string> Valid values are ACLWithLD APEmailFm t , ACLWithMa nualEmailFmt , or ACLWithUs ernameFmt .	No
proxyHost	The host where the web proxy is required. The host name should be without protocol (http:// or https://).	string	Yes
proxyPort	Port used by the host URL transport protocol. The port number should be a numeric value between 0 and 65535.	string	Yes

Configuration	Description	Type	Required
• crawlAcl • crawlFiles • crawlPages • crawlEvents • crawlComments • crawlLinks • crawlAttachments • crawlListData • isCrawlLocalGroupMapping • isCrawlAdGroupMapping	Input TRUE to index.	boolean	No
maxFileSizeInMegaBytes	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	string	No

Configuration	Description	Type	Required
`sslCertificatePath`	Configuration information to access the SSL certificate stored in your Amazon S3 bucket.	`object` This property has the following sub-properties. • `bucket` • `key`	No
`bucket`	The name of the Amazon S3 bucket that stores your Microsoft Entra ID (formerly Azure AD) self-signed X.509 certificate.	`string`	Yes
`key`	The name of the SSL certificate stored in your Amazon S3 bucket.	`string`	Yes
`type`	We recommend that you use `SHAREPOINTV2` as your data source type.	`string` Valid values are `SHAREPOINTV2` and `SHAREPOINT`.	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. See Identity crawler for more information.	`boolean`	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index	Yes

Configuration	Description	Type	Required
secretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your SharePoint. If you use OAuth2App authentication, provide the client ID, client secret, LDAP URL, LDAP base DN, LDAP user name, and LDAP password. If you use NTLM or Kerberos authentication, provide the user name, password, LDAP URL, Base DN, LDAP user, and LDAP password.	string The minimum length is 20 and the maximum length is 2,048 characters. If you use Sharepoint App-Only authentication (authType should be 0Auth2App authentication) the secret must contain a JSON structure with the following keys: { "clientId": "*client ID*", "clientSecret": " *client secret*", "ldapUrl": "*LDAP URL*", "ldbaseDn": "*LDAP base DN*", "ldapUser": " *LDAP user name*", "ldapPassword": " *LDAP password*" } If you use NTLM authentication or Kerberos authentic	Yes

Configuration	Description	Type	Required
		ation, the secret must contain a JSON structure with the following keys: `{ "userName": "SharePoint account user name", "password": " SharePoint account password", "ldapUrl": "LDAP URL", "baseDn": "LDAP base DN", "ldapUser": " LDAP user name", "ldapPassword": " LDAP password" }`	
`version`	The version of this template that&s currently supported.	`string`	No

SharePoint Server 2016 JSON schema

The following is the SharePoint Server 2016 JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
```

```
      "enum": ["SHAREPOINTV2", "SHAREPOINT"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "sslCertificatePath": {
      "type": "object",
      "properties": {
        "bucket": {
          "type": "string",
          "pattern": "^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$",
          "minLength": 3,
          "maxLength": 63
        },
        "key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 10240
        }
      },
      "required": ["bucket", "key"]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
```

```
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            },
            "domain": {
              "type": "string"
            },
            "siteUrls": {
              "type": "array",
              "items": {
                "type": "string",
                "pattern": "https://.*"
              }
            },
            "repositoryAdditionalProperties": {
              "type": "object",
              "properties": {
                "authType": {
                  "type": "string",
                  "enum": ["OAuth2App", "NTLM", "Kerberos"]
                },
                "version": {
                  "type": "string",
                  "enum": ["Server"]
                },
                "onPremVersion": {
                  "type": "string",
                  "enum": ["", "2013", "2016", "2019", "SubscriptionEdition"]
                },
                "enableDeletionProtection": {
                  "anyOf": [
                    {
                      "type": "boolean"
                    },
                    {
                      "type": "string",
                      "enum": ["true", "false"]
                    }
                  ],
                  "default": false
```

```
              },
              "deletionProtectionThreshold": {
                "type": "string",
                "default": "15"
              }
            },
            "required": ["authType", "version"]
          }
        },
        "required": ["siteUrls", "domain", "repositoryAdditionalProperties"]
      }
    },
    "required": ["repositoryEndpointMetadata"]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "event": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
```

```
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "page": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "file": {
```

```
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "link": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "attachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
```

```
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "comment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
```

```
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "eventTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "pageTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "linkTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionFilePath": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionFilePath": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionFileTypePatterns": {
        "type": "array",
```

```
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionOneNoteSectionNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionOneNoteSectionNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionOneNotePageNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionOneNotePageNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
```

```
          }
        },
        "crawlFiles": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlPages": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlEvents": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlComments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
```

```
          ]
        },
        "crawlLinks": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAttachments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlListData": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
```

```
          ]
        },
        "aclConfiguration": {
          "type": "string",
          "enum": [
            "ACLWithLDAPEmailFmt",
            "ACLWithManualEmailFmt",
            "ACLWithUsernameFmt"
          ]
        },
        "emailDomain": {
          "type": "string"
        },
        "isCrawlLocalGroupMapping": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlAdGroupMapping": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "proxyHost": {
          "type": "string"
        },
        "proxyPort": {
          "type": "string"
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        }
```

```
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "type",
    "secretArn",
    "syncMode",
    "enableIdentityCrawler",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

SharePoint Server 2016 JSON schema example

The following is the SharePoint Server 2016 JSON schema example:

```
{

  "type": "SHAREPOINTV2",

  "syncMode": "FULL_CRAWL",

  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-sharepoint-
secret",

  "enableIdentityCrawler": "true",

  "sslCertificatePath": {

    "bucket": "my-sharepoint-bucket",

    "key": "ssl/cert.pem"
```

```
  },
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "tenantId": "1234567a-890b-1234-567c-123456789012",
      "domain": "mycompany.sharepoint.com",
      "siteUrls": [
        "https://mycompany.sharepoint.com/sites/TeamSite"
      ],
      "repositoryAdditionalProperties": {
        "authType": "OAuth2",
        "version": "Server",
        "onPremVersion": "2019",
        "enableDeletionProtection": "false",
        "deletionProtectionThreshold": "15"
      }
    }
  },
  "repositoryConfigurations": {
    "event": {
      "fieldMappings": [
        {
          "indexFieldName": "event_id",
          "indexFieldType": "STRING",
```

```
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    ]
  },
  "page": {
    "fieldMappings": [
      {
        "indexFieldName": "page_id",
        "indexFieldType": "STRING",
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    ]
  },
  "file": {
    "fieldMappings": [
      {
        "indexFieldName": "file_id",
        "indexFieldType": "STRING",
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
```

```
        }
      ]
    },
    "link": {
      "fieldMappings": [
        {
          "indexFieldName": "link_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "attachment": {
      "fieldMappings": [
        {
          "indexFieldName": "attachment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
```

```
    },

    "comment": {

      "fieldMappings": [

        {

          "indexFieldName": "comment_id",

          "indexFieldType": "STRING",

          "dataSourceFieldName": "id",

          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"

        }

      ]

    }

  },

  "additionalProperties": {

    "eventTitleFilterRegEx": [
      "^.*$"
    ],

    "pageTitleFilterRegEx": [
      "^.*$"
    ],

    "linkTitleFilterRegEx": [
      "^.*$"
    ],

    "inclusionFilePath": [
      "documents/"
    ],

    "exclusionFilePath": [
      "drafts/"
```

```
    ],

    "inclusionFileTypePatterns": [
      "*.pdf",
       "*.docx"
    ],

    "exclusionFileTypePatterns": [
      "*.tmp"
    ],

    "inclusionFileNamePatterns": [
      "*report*"
    ],

    "exclusionFileNamePatterns": [
      "*draft*"
    ],

    "inclusionOneNoteSectionNamePatterns": [
      "*"
    ],

    "exclusionOneNoteSectionNamePatterns": [
      "archived"
    ],

    "inclusionOneNotePageNamePatterns": [
      "*"
    ],

    "exclusionOneNotePageNamePatterns": [
      "test"
    ],

    "crawlFiles": "true",

    "crawlPages": "true",

    "crawlEvents": "true",

    "crawlComments": "true",

    "crawlLinks": "true",
```

```
    "crawlAttachments": "true",
    "crawlListData": "false",
    "crawlAcl": "true",
    "aclConfiguration": "ACLWithUsernameFmt",
    "emailDomain": "mycompany.com",
    "isCrawlLocalGroupMapping": "false",
    "isCrawlAdGroupMapping": "true",
    "proxyHost": "proxy.mycompany.com",
    "proxyPort": "8080",
    "maxFileSizeInMegaBytes": "50"
  },
  "version": "1.0.0"
}
```

Connecting Amazon Q Business to SharePoint Server 2016 using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- SharePoint Server 2016 configuration properties
- SharePoint Server 2016 JSON schema for using the configuration property with AWS CloudFormation

- SharePoint Server 2016 YAML schema for using the configuration property with AWS CloudFormation

SharePoint Server 2016 configuration properties

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-properties. • `siteUrls` • `domain` • `repositoryAdditionalProperties` • `tenantId`	Yes
`tenantId`	The tenant id of your SharePoint account.	`string` OAuth2 series required	Yes
`domain`	The domain of your SharePoint account.	`string`	Yes

Configuration	Description	Type	Required
`siteUrls`	The host URLs of your SharePoint account.	`array (string)` Specify the URL in the pattern `https://*`	Yes
`repositoryAdditionalProperties`	Additional properties to connect with your repository endpoint.	`object` This property has the following sub-properties. • `version` • `authType` • `onPremVersion`	Yes
`authType`	The type of authentication you are using: `NTLM`, `Kerberos`, or `OAuth2App` .	`string`	Yes
`version`	The SharePoint version you are using: `Sever`.	`string (Server)`	Yes
`onPremVersion`	The SharePoint version that you are using.	`string` Valid values are (empty), `2013`, `2016`, `2019`, and `SubscriptionEdition` .	Yes

Configuration	Description	Type	Required
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties. • `event` • `page` • `file` • `link` • `attachment` • `comment`	Yes
• `event` • `page` • `file` • `link` • `attachment` • `comment`	A list of objects that map the attributes or field names of your SharePoint Server 2016 pages and assets to Amazon Q index field names.	`object` These properties have the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName` • `dateFieldFormat`	No
`indexFieldName`	The field name of your SharePoint Server 2016 events, pages, files, links, attachments, or comments.	`string`	Yes

Configuration	Description	Type	Required
`indexFieldType`	The field type of your SharePoint Server 2016 events, pages, files, links, attachments, or comments.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes
`dataSourceFieldName`	The data source field name of your SharePoint Server 2016 events, pages, files, links, attachments, or comments.	`string`	Yes
`dateFieldFormat`	The date format of your SharePoint Server 2016 events, pages, files, links, attachments, or comments.	`string` Specify the date format in the form `yyyy-MM-dd"T"HH:mm:ss"Z"`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties: • crawlAcl • crawlFiles • crawlPages • crawlEvents • crawlComments • crawlLinks • crawlAttachments • crawlListData • isCrawlLocalGroupMapping • isCrawlAdGroupMapping • aclConfiguration • emailDomain • maxFileSizeInMegaBytes • eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx	Yes

Configuration	Description	Type	Required
		• inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotePageNamePatterns	

Configuration	Description	Type	Required
		• `proxyHost` • `proxyPort`	

Configuration	Description	Type	Required
• eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePa	A list of regular expression patterns to include/exclude specific files in your SharePoint data source. Files that match the patterns are included in the index. File that don&t match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn&t included in the index.	array (string)	No

Configuration	Description	Type	Required
geNamePat terns • exclusion OneNotePa geNamePat terns • emailDomain			
aclConfig uration	Specifes how your ACL is configured.	string> Valid values are ACLWithLD APEmailFm t , ACLWithMa nualEmailFmt , or ACLWithUs ernameFmt .	No
proxyHost	The host where the web proxy is required. The host name should be without protocol (http:// or https://).	string	Yes
proxyPort	Port used by the host URL transport protocol. The port number should be a numeric value between 0 and 65535.	string	Yes

Configuration	Description	Type	Required
• crawlAcl • crawlFiles • crawlPages • crawlEvents • crawlComments • crawlLinks • crawlAttachments • crawlListData • isCrawlLocalGroupMapping • isCrawlAdGroupMapping	Input TRUE to index.	boolean	No
maxFileSizeInMegaBytes	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	string	No

Configuration	Description	Type	Required
`sslCertificatePath`	Configuration information to access the SSL certificate stored in your Amazon S3 bucket.	`object` This property has the following sub-properties. • `bucket` • `key`	No
`bucket`	The name of the Amazon S3 bucket that stores your Microsoft Entra ID (formerly Azure AD) self-signed X.509 certificate.	`string`	Yes
`key`	The name of the SSL certificate stored in your Amazon S3 bucket.	`string`	Yes
`type`	We recommend that you use `SHAREPOINTV2` as your data source type.	`string` Valid values are `SHAREPOINTV2` and `SHAREPOINT`.	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. See Identity crawler for more information.	`boolean`	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index	Yes

Configuration	Description	Type	Required
secretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your SharePoint. If you use OAuth2App authentication, provide the client ID, client secret, LDAP URL, LDAP base DN, LDAP user name, and LDAP password. If you use NTLM or Kerberos authentication, provide the user name, password, LDAP URL, Base DN, LDAP user, and LDAP password.	string The minimum length is 20 and the maximum length is 2,048 characters. If you use Sharepoint App-Only authentication (authType should be 0Auth2App authentication) the secret must contain a JSON structure with the following keys: { "clientId": "*client ID*", "clientSecret": " *client secret*", "ldapUrl": "*LDAP URL*", "ldbaseDn": "*LDAP base DN*", "ldapUser": " *LDAP user name*", "ldapPassword": " *LDAP password*" } If you use NTLM authentication or Kerberos authentic	Yes

Configuration	Description	Type	Required
		ation, the secret must contain a JSON structure with the following keys: `{ "userName": "SharePoint account user name", "password": " SharePoint account password", "ldapUrl": "LDAP URL", "baseDn": "LDAP base DN", "ldapUser": " LDAP user name", "ldapPassword": " LDAP password" }`	
`version`	The version of this template that&s currently supported.	`string`	No

SharePoint Server 2016 JSON schema for using the configuration property with AWS CloudFormation

The following is the SharePoint Server 2016 JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- SharePoint Server 2016 JSON schema for using the configuration property with AWS CloudFormation
- SharePoint Server 2016 JSON schema example for using the configuration property with AWS CloudFormation

SharePoint Server 2016 JSON schema for using the configuration property with AWS CloudFormation

The following is the SharePoint Server 2016 JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["SHAREPOINTV2", "SHAREPOINT"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "sslCertificatePath": {
      "type": "object",
      "properties": {
        "bucket": {
```

```
          "type": "string",
          "pattern": "^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$",
          "minLength": 3,
          "maxLength": 63
        },
        "key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 10240
        }
      },
      "required": ["bucket", "key"]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            },
            "domain": {
              "type": "string"
            },
            "siteUrls": {
              "type": "array",
              "items": {
                "type": "string",
                "pattern": "https://.*"
              }
            },
            "repositoryAdditionalProperties": {
              "type": "object",
              "properties": {
                "authType": {
                  "type": "string",
                  "enum": ["OAuth2App", "NTLM", "Kerberos"]
                },
                "version": {
```

```
                "type": "string",
                "enum": ["Server"]
              },
              "onPremVersion": {
                "type": "string",
                "enum": ["", "2013", "2016", "2019", "SubscriptionEdition"]
              },
              "enableDeletionProtection": {
                "anyOf": [
                  {
                    "type": "boolean"
                  },
                  {
                    "type": "string",
                    "enum": ["true", "false"]
                  }
                ],
                "default": false
              },
              "deletionProtectionThreshold": {
                "type": "string",
                "default": "15"
              }
            },
            "required": ["authType", "version"]
          }
        },
        "required": ["siteUrls", "domain", "repositoryAdditionalProperties"]
      }
    },
    "required": ["repositoryEndpointMetadata"]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "event": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
```

```
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "page": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
```

```
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "file": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
```

```
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "link": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "attachment": {
```

```
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "comment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "eventTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "pageTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "linkTitleFilterRegEx": {
        "type": "array",
```

```
          "items": {
            "type": "string"
          }
        },
        "inclusionFilePath": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFilePath": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionOneNoteSectionNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
```

```
        }
      },
      "exclusionOneNoteSectionNamePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionOneNotePageNamePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionOneNotePageNamePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "crawlFiles": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlPages": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlEvents": {
        "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlComments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlLinks": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAttachments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlListData": {
          "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "aclConfiguration": {
          "type": "string",
          "enum": [
            "ACLWithLDAPEmailFmt",
            "ACLWithManualEmailFmt",
            "ACLWithUsernameFmt"
          ]
        },
        "emailDomain": {
          "type": "string"
        },
        "isCrawlLocalGroupMapping": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlAdGroupMapping": {
          "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "proxyHost": {
          "type": "string"
        },
        "proxyPort": {
          "type": "string"
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "type",
    "secretArn",
    "syncMode",
    "enableIdentityCrawler",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

SharePoint Server 2016 JSON schema example for using the configuration property with AWS CloudFormation

The following is the SharePoint Server 2016 JSON schema example for the configuration property for CloudFormation

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation SHAREPOINT Data Source Template",
  "Resources": {
    "DataSourceSharePoint": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MySharePointDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "SHAREPOINTV2",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-
sharepoint-secret",
          "enableIdentityCrawler": "true",
          "sslCertificatePath": {
            "bucket": "my-sharepoint-bucket",
```

```
            "key": "ssl/cert.pem"

          },

          "connectionConfiguration": {

            "repositoryEndpointMetadata": {

              "tenantId": "1234567a-890b-1234-567c-123456789012",

              "domain": "mycompany.sharepoint.com",

              "siteUrls": [
                "https://mycompany.sharepoint.com/sites/TeamSite"
              ],

              "repositoryAdditionalProperties": {

                "authType": "OAuth2",

                "version": "Server",

                "onPremVersion": "2019",

                "enableDeletionProtection": "false",

                "deletionProtectionThreshold": "15"

              }

            }

          },

          "repositoryConfigurations": {

            "event": {

              "fieldMappings": [

                {

                  "indexFieldName": "event_id",
```

```
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "page": {
        "fieldMappings": [
          {
            "indexFieldName": "page_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "file": {
        "fieldMappings": [
          {
            "indexFieldName": "file_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
```

```
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "link": {
        "fieldMappings": [
          {
            "indexFieldName": "link_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "attachment": {
        "fieldMappings": [
          {
            "indexFieldName": "attachment_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
```

```
            ]

          },

          "comment": {

            "fieldMappings": [

              {

                "indexFieldName": "comment_id",

                "indexFieldType": "STRING",

                "dataSourceFieldName": "id",

                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"

              }

            ]

          }

        },

        "additionalProperties": {

          "eventTitleFilterRegEx": [
            "^.*$"
          ],

          "pageTitleFilterRegEx": [
            "^.*$"
          ],

          "linkTitleFilterRegEx": [
            "^.*$"
          ],

          "inclusionFilePath": [
            "documents/"
          ],
```

```
            "exclusionFilePath": [
              "drafts/"
            ],

            "inclusionFileTypePatterns": [
              "*.pdf",
               "*.docx"
            ],

            "exclusionFileTypePatterns": [
              "*.tmp"
            ],

            "inclusionFileNamePatterns": [
              "*report*"
            ],

            "exclusionFileNamePatterns": [
              "*draft*"
            ],

            "inclusionOneNoteSectionNamePatterns": [
              "*"
            ],

            "exclusionOneNoteSectionNamePatterns": [
              "archived"
            ],

            "inclusionOneNotePageNamePatterns": [
              "*"
            ],

            "exclusionOneNotePageNamePatterns": [
              "test"
            ],

            "crawlFiles": "true",

            "crawlPages": "true",

            "crawlEvents": "true",

            "crawlComments": "true",
```

```
            "crawlLinks": "true",
            "crawlAttachments": "true",
            "crawlListData": "false",
            "crawlAcl": "true",
            "aclConfiguration": "ACLWithUsernameFmt",
            "emailDomain": "mycompany.com",
            "isCrawlLocalGroupMapping": "false",
            "isCrawlAdGroupMapping": "true",
            "proxyHost": "proxy.mycompany.com",
            "proxyPort": "8080",
            "maxFileSizeInMegaBytes": "50"
          }
        }
      }
    }
  }
}
```

SharePoint Server 2016 YAML schema for using the configuration property with AWS CloudFormation

The following is the SharePoint Server 2016 YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- SharePoint Server 2016 YAML schema for using the configuration property with AWS CloudFormation
- SharePoint Server 2016 YAML schema example for using the configuration property with AWS CloudFormation

SharePoint Server 2016 YAML schema for using the configuration property with AWS CloudFormation

The following is the SharePoint Server 2016 YAML schema for the configuration property for CloudFormation.

```
type: object
properties:
  type:
    type: string
    enum:
      - SHAREPOINTV2
      - SHAREPOINT
  syncMode:
    type: string
    enum:
      - FULL_CRAWL
      - FORCED_FULL_CRAWL
      - CHANGE_LOG
  secretArn:
    type: string
    minLength: 20
    maxLength: 2048
  enableIdentityCrawler:
    anyOf:
      - type: boolean
      - type: string
        enum:
          - true
          - false
  sslCertificatePath:
    type: object
    properties:
      bucket:
        type: string
        pattern: '^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$'
        minLength: 3
```

```
        maxLength: 63
      key:
        type: string
        minLength: 1
        maxLength: 10240
    required:
      - bucket
      - key
  connectionConfiguration:
    type: object
    properties:
      repositoryEndpointMetadata:
        type: object
        properties:
          tenantId:
            type: string
            pattern: "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$"
            minLength: 36
            maxLength: 36
          domain:
            type: string
          siteUrls:
            type: array
            items:
              type: string
              pattern: "https://.*"
          repositoryAdditionalProperties:
            type: object
            properties:
              authType:
                type: string
                enum:
                  - OAuth2App
                  - NTLM
                  - Kerberos
              version:
                type: string
                enum:
                  - Server
              onPremVersion:
                type: string
                enum:
                  - ""
                  - "2013"
```

```
                - "2016"
                - "2019"
                - SubscriptionEdition
            enableDeletionProtection:
              anyOf:
                - type: boolean
                - type: string
                  enum:
                    - true
                    - false
              default: false
            deletionProtectionThreshold:
              type: string
              default: "15"
          required:
            - authType
            - version
      required:
        - siteUrls
        - domain
        - repositoryAdditionalProperties
  required:
    - repositoryEndpointMetadata
repositoryConfigurations:
  type: object
  properties:
    event:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
```

```
            dateFieldFormat:
              type: string
              pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
          required:
            - indexFieldName
            - indexFieldType
            - dataSourceFieldName
      required:
        - fieldMappings
    page:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - DATE
                  - LONG
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    file:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
```

```
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - DATE
                  - LONG
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
        required:
          - fieldMappings
      link:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
```

```
        required:
          - fieldMappings
      attachment:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      comment:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
```

```
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
  required: []
additionalProperties:
  type: object
  properties:
    eventTitleFilterRegEx:
      type: array
      items:
        type: string
    pageTitleFilterRegEx:
      type: array
      items:
        type: string
    linkTitleFilterRegEx:
      type: array
      items:
        type: string
    inclusionFilePath:
      type: array
      items:
        type: string
    exclusionFilePath:
      type: array
      items:
        type: string
    inclusionFileTypePatterns:
      type: array
      items:
        type: string
    exclusionFileTypePatterns:
      type: array
      items:
        type: string
```

```
      inclusionFileNamePatterns:
        type: array
        items:
          type: string
      exclusionFileNamePatterns:
        type: array
        items:
          type: string
      inclusionOneNoteSectionNamePatterns:
        type: array
        items:
          type: string
      exclusionOneNoteSectionNamePatterns:
        type: array
        items:
          type: string
      inclusionOneNotePageNamePatterns:
        type: array
        items:
          type: string
      exclusionOneNotePageNamePatterns:
        type: array
        items:
          type: string
      crawlFiles:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlPages:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlEvents:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
```

```
            - false
      crawlComments:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlLinks:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlAttachments:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlListData:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlAcl:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      aclConfiguration:
        type: string
        enum:
          - ACLWithLDAPEmailFmt
          - ACLWithManualEmailFmt
          - ACLWithUsernameFmt
      emailDomain:
        type: string
```

```
      isCrawlLocalGroupMapping:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      isCrawlAdGroupMapping:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      proxyHost:
        type: string
      proxyPort:
        type: string
      maxFileSizeInMegaBytes:
        type: string
    required: []
  version:
    type: string
    anyOf:
      - pattern: 1.0.0
required:
  - type
  - secretArn
  - syncMode
  - enableIdentityCrawler
  - connectionConfiguration
  - repositoryConfigurations
  - additionalProperties
```

SharePoint Server 2016 YAML schema example for using the configuration property with AWS CloudFormation

The following is the SharePoint Server 2016 YAML example for the Configuration property for CloudFormation:

```
{
```

```
  "type": "SHAREPOINTV2",

  "syncMode": "FULL_CRAWL",

  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-sharepoint-
secret",

  "enableIdentityCrawler": "true",

  "sslCertificatePath": {

    "bucket": "my-sharepoint-bucket",

    "key": "ssl/cert.pem"

  },

  "connectionConfiguration": {

    "repositoryEndpointMetadata": {

      "tenantId": "1234567a-890b-1234-567c-123456789012",

      "domain": "mycompany.sharepoint.com",

      "siteUrls": [
        "https://mycompany.sharepoint.com/sites/TeamSite"
      ],

      "repositoryAdditionalProperties": {

        "authType": "OAuth2",

        "version": "Server",

        "onPremVersion": "2019",

        "enableDeletionProtection": "false",

        "deletionProtectionThreshold": "15"

      }

    }
```

```
},
"repositoryConfigurations": {
  "event": {
    "fieldMappings": [
      {
        "indexFieldName": "event_id",
        "indexFieldType": "STRING",
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    ]
  },
  "page": {
    "fieldMappings": [
      {
        "indexFieldName": "page_id",
        "indexFieldType": "STRING",
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    ]
  },
```

```
    "file": {
      "fieldMappings": [
        {
          "indexFieldName": "file_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "link": {
      "fieldMappings": [
        {
          "indexFieldName": "link_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "attachment": {
      "fieldMappings": [
```

```
        {
          "indexFieldName": "attachment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "comment": {
      "fieldMappings": [
        {
          "indexFieldName": "comment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    }
  },
  "additionalProperties": {
    "eventTitleFilterRegEx": [
      "^.*$"
    ],
```

```
    "pageTitleFilterRegEx": [
      "^.*$"
    ],

    "linkTitleFilterRegEx": [
      "^.*$"
    ],

    "inclusionFilePath": [
      "documents/"
    ],

    "exclusionFilePath": [
      "drafts/"
    ],

    "inclusionFileTypePatterns": [
      "*.pdf",
       "*.docx"
    ],

    "exclusionFileTypePatterns": [
      "*.tmp"
    ],

    "inclusionFileNamePatterns": [
      "*report*"
    ],

    "exclusionFileNamePatterns": [
      "*draft*"
    ],

    "inclusionOneNoteSectionNamePatterns": [
      "*"
    ],

    "exclusionOneNoteSectionNamePatterns": [
      "archived"
    ],

    "inclusionOneNotePageNamePatterns": [
      "*"
```

```
    ],

    "exclusionOneNotePageNamePatterns": [
      "test"
    ],

    "crawlFiles": "true",

    "crawlPages": "true",

    "crawlEvents": "true",

    "crawlComments": "true",

    "crawlLinks": "true",

    "crawlAttachments": "true",

    "crawlListData": "false",

    "crawlAcl": "true",

    "aclConfiguration": "ACLWithUsernameFmt",

    "emailDomain": "mycompany.com",

    "isCrawlLocalGroupMapping": "false",

    "isCrawlAdGroupMapping": "true",

    "proxyHost": "proxy.mycompany.com",

    "proxyPort": "8080",

    "maxFileSizeInMegaBytes": "50"

  },

  "version": "1.0.0"

}
```

How Amazon Q Business connector crawls SharePoint Server 2016 ACLs

When you connect an SharePoint Server 2016 data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your SharePoint Server 2016 instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

To filter using a username, use the **User principal name** from your Azure portal. For example, johnstiles@kendra.onmicrosoft.com.

When you use a SharePoint group for user context filtering, calculate the group ID as follows:

For local groups

1. Get the site name. For example, `https://host.onmicrosoft.com/sites/siteName`.
2. Take the SHA256 hash of the site name. For example, `430a6b90503eef95c89295c8999c7981`.
3. Create the group ID by concatenating the SHA256 hash with a vertical bar (|) and the group name. For example, if the group name is "local group name", the group ID is the following:

   `"430a6b90503eef95c89295c8999c7981 | localGroupName"` (with a space before and after the vertical bar).

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Amazon Q Business SharePoint Server 2016 data source connector field mappings

To help you structure data for retrieval and chat filtering, Amazon Q Business crawls data source document attributes or metadata and maps them to fields in your Amazon Q index.

Amazon Q has reserved fields that it uses when querying your application. When possible, Amazon Q automatically maps these built-in fields to attributes in your data source. If a built-in field doesn't have a default mapping, or if you want to map additional index fields, use the custom field mappings to specify how a data source attribute maps to your Amazon Q application. You create

field mappings by editing your data source after your application environment and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Sharepoint connector supports the following entities and the associated reserved and custom attributes.

> **Important**
>
> If you map any SharePoint Server 2016 field to Amazon Q document title and document body fields, Amazon Q will generate responses from data in the document title and body.

> **Note**
>
> You can map any Sharepoint field to the document title or document body Amazon Q reserved/default index fields.

Supported entities and field mappings

- Files
- Events
- Pages
- Links
- Attachments
- Comments

Files

Sharepoint field name	Index field name	Description	Data type
title	sp_title	Custom	String
sourceUri	_source_uri	Default	String
checkInComment	sp_checkInComment	Custom	String
size	sp_sizeLong	Custom	Long (numeric)
lastModifiedDateTime	_last_updated_at	Default	Date
createdAt	_created_at	Default	Date
author	_authors	Default	String list
majorVersion	sp_majorVersion	Custom	String
uiVersionLabel	sp_uiVersionLabel	Custom	String
uniqueId	sp_uniqueId	Custom	String
irmEnabled	sp_irmEnabled	Custom	String
checkOutType	sp_checkOutType	Custom	String
category	_category	Default	String
modifiedBy	sp_modifiedBy	Custom	String
level	sp_level	Custom	String
uiVersion	sp_uiVersion	Custom	String
contentTag	sp_contentTag	Custom	String
eTag	sp_eTag	Custom	String

Sharepoint field name	Index field name	Description	Data type
oneNoteDocument	sp_oneNoteDocument	Custom	String
oneNoteSection	sp_oneNoteSection	Custom	String
oneNotePage	sp_oneNotePage	Custom	String

Events

Sharepoint field name	Index field name	Description	Data type
title	sp_title	Custom	String
lastModifiedDateTime	_last_updated_at	Default	Date
sourceUri	_source_uri	Default	String
attachments	sp_hasAttachments	Custom	String
createdDate	_created_at	Default	Date
authorId	sp_authorId	Custom	String
editorId	sp_editorId	Custom	String
location	sp_location	Custom	String
eventDate	sp_eventDate	Custom	Date
eventEndDate	sp_eventEndDate	Custom	Date
ifRecurrence	sp_ifRecurrence	Custom	String
ifAllDayEvent	sp_ifAllDayEvent	Custom	String

Sharepoint field name	Index field name	Description	Data type
category	_category	Default	String
eventCategory	sp_eventcategory	Custom	String

Pages

Sharepoint field name	Index field name	Description	Data type
createdDateTime	_created_at	Default	Date
lastModifiedDateTime	_last_updated_at	Default	Date
title	sp_title	Custom	String
sourceUri	_source_uri	Default	String
firstPublishedDate	sp_firstPublishedDate	Custom	Date
authorId	sp_authorId	Custom	String
editorId	sp_editorId	Custom	String
category	_category	Default	String

Links

Sharepoint field name	Index field name	Description	Data type
createdAt	_created_at	Default	Date
lastModifiedDateTime	_last_updated_at	Default	Date

Sharepoint field name	Index field name	Description	Data type
title	sp_title	Custom	String
sourceUri	_source_uri	Default	String
fileType	sp_fileType	Custom	String
fileDirPath	sp_fileDirPath	Custom	String
firstPublishedDate	sp_firstPublishedDate	Custom	Date
authorId	sp_authorId	Custom	String
editorId	sp_editorId	Custom	String
category	_category	Default	String
size	sp_sizeLong	Custom	Long (numeric)

Attachments

Sharepoint field name	Index field name	Description	Data type
title	sp__title	Custom	String
parentCreatedDate	_created_at	Default	Date
sourceUri	_source_uri	Default	String
parentModifiedDate	_last_updated_at	Custom	Date
parentListId	sp_parentListId	Custom	String
parentTitle	sp_parentTitle	Custom	String
category	_category	Default	String

Comments

Sharepoint field name	Index field name	Description	Data type
createdDateTime	_created_at	Default	Date
likedBy	sp_likedBy	Custom	String
sourceUri	_source_uri	Custom	String
isReply	sp_isReply	Custom	String
author	_authors	Default	String list
listId	sp_listId	Custom	String
category	_category	Default	String
replyCount	sp_replyCount	Custom	String
parentTitle	sp_parentTitle	Custom	String

IAM role for Amazon Q Business SharePoint Server 2016 connector

> **Note**
>
> **(Optional)** If you use **Azure App-Only authentication**, you also need to add permissions for Amazon Q to access the certificate stored in your Amazon S3 bucket.

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
```

```
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the SharePoint Server 2016 connector

The following table provides information about error codes you may see for the Microsoft SharePoint connector and suggested resolutions.

Error code	Error message	Suggested resolution
SPE-5001	Authentication failed. Configuration might contain wrong credentia ls.	Provide valid credentials like username, password or client Id, client secret and tenant Id.
SPE-5002	There was a problem while connecting to Host Url and/or Domain. hostUrl and/or domain	Provide valid Host URL or Domain.

Error code	Error message	Suggested resolution
	values might be incorrect .	
SPE-5003	Provided URL is incorrect	Provide correct URL.
SPE-5004	Inet Address validation Failed.	Provide valid Inet Address
SPE-5005	Failed : HTTP protocol violation has occurred.	Try running the connector again.
SPE-5006	Cannot connect to proxy. Check the proxy configurations.	Provide valid Proxy configuration details.
SPE-5007	Proxy port is invalid. Check the proxy port.	Provide valid Proxy port.
SPE-5008	Valid SSL Certificate could not be found for connector.	Provide valid SSL certificate.
SPE-5009	There was a problem while connecting to LDAP. Check LDAP configuration.	Provide valid LDAP configuration details.
SPE-5100	There was a problem while retrieving repositor yId. Repository ID might be empty or null.	Ensure that repository Id must not be null or empty.

Error code	Error message	Suggested resolution
SPE-5101	There was a problem while retrieving dataSourceIamRoleArn. Data Source IAM Role ARN might be empty or null.	Ensure that dataSourceIamRoleArn must not be null or empty.
SPE-5102	There was a problem while retrieving repository configurations. Repository configurations might be empty or incorrect.	Provide valid repository configurations.
SPE-5115	There was a problem while retrieving field mapping values for event entity. Field mapping values might be empty or incorrect.	Field mapping values for event entity should be correct or non-empty.
SPE-5116	There was a problem while retrieving field mapping values for file entity. Field mapping values might be empty or incorrect.	Field mapping values for file entity should be correct or non-empty.
SPE-5117	There was a problem while retrieving field mapping values for page entity. Field mapping values might be empty or incorrect.	Field mapping values for page entity should be correct or non-empty.

Error code	Error message	Suggested resolution
SPE-5118	There was a problem while retrieving field mapping values for link entity. Field mapping values might be empty or incorrect.	Field mapping values for link entity should be correct or non-empty.
SPE-5119	There was a problem while retrieving field mapping values for comment entity. Field mapping values might be empty or incorrect.	Field mapping values for comment entity should be correct or non-empty.
SPE-5120	There was a problem while retrieving field mapping values for attachment entity. Field mapping values might be empty or incorrect.	Field mapping values for attachment entity should be correct or non-empty.
SPE-5121	There was a problem while retrieving values for crawl entities. Values might be empty or incorrect. It should be either true or false.	There might be some incorrect value given in any one of the crawling entities like – null, TRUE or any dummy string. Ensure the value must be non-empty and either true or false.
SPE-5122	There was a problem while retrieving domain. Domain might be empty or null.	Provide Client Id.

Error code	Error message	Suggested resolution
SPE-5123	There was a problem while retrieving version. Version might be empty or null.	Provide valid version and it should not be null.
SPE-5124	There was a problem while retrieving authType. Auth-Type might be empty or null.	Ensure AUTH Type in configuration must be not null.
SPE-5125	There was a problem while retrieving clientId. Client ID might be empty or null.	Provide Client Id.
SPE-5126	There was a problem while retrieving clientSecret. Client Secret might be empty or null.	Provide Client Secret.
SPE-5127	There was a problem while retrieving tenantId. Tenant ID might be empty or null.	Provide Tenant Id.
SPE-5128	There was a problem while retrieving siteUrls. Site URLs might be empty or null.	Provide at least one Site Url.
SPE-5129	There was a problem while retrieving password. Password might be empty or null.	Provide password.

Error code	Error message	Suggested resolution
SPE-5130	There was a problem while retrieving username.Username might be empty or null.	Provide username.
SPE-5131	There was a problem while retrieving username. Email was invalid.	Provide valid email address.
SPE-5132	There was a problem while retrieving url. This URL was invalid.	Provide a valid URL.
SPE-5133	There was a problem while retrieving s3CertificateName. S3 Certificate Name might be empty or null.	Ensure s3CertificateName is not null or non-empty.
SPE-5134	There was a problem while retrieving s3BucketName. S3 Bucket Name might be empty or null	Ensure s3BucketName is not null or non-empty.
SPE-5135	The provided version was not a valid Sharepoint Connector version. Version should be one of [Online, Server].	Version should be one of [Online, Server].
SPE-5136	The provided authType was not a valid Sharepoint Connector authentication method.	Provide valid authType. The value of authType should be one of [Basic, OAuth2Certificate, OAuth2].

Error code	Error message	Suggested resolution
SPE-5138	There was a problem while retrieving onPremVersion. On prem Version might be empty or null	Ensure onPremVersion is not be null or non-empty.
SPE-5139	The provided onPremVersion was not valid Sharepoint on-prem version. On prem version should be one of [2013, 2016, 2019, SubscriptionEdition].	Provide a valid onPremVersion. On prem version should be one of [2013, 2016, 2019, SubscriptionEdition].
SPE-5140	There was a problem while retrieving ldapUrl. LDAP Url might be empty or null.	Ensure ldapUrl is not null or empty.
SPE-5141	There was a problem while retrieving baseDn. Base DN might be empty or null.	Ensure baseDn is not be null or empty.
SPE-5142	There was a problem while retrieving privateKey. Private Key might be empty or null.	Please ensure privateKey is not be null or empty.
SPE-5144	There was a problem while retrieving aclConfiguration. ACL Configuration might be empty, null or invalid	Provide valid aclConfiguration. aclConfiguration should be one of [ACLWithLDAPEmailFmt, ACLWithManualEmailFmt, ACLWithUsernameFmt].

Error code	Error message	Suggested resolution
SPE-5145	There was a problem while retrieving emailDomain. Email Domain might be empty or null.	Ensure emailDomain is not null or empty.
SPE-5146	There was a problem while retrieving ldapUsername. LDAP Username might be empty or null.	Ensure ldapUser is not null or empty.
SPE-5147	There was a problem while retrieving ldapPassword. LDAP Password might be empty or null.	Ensure ldapPassword is not null or empty.
SPE-5149	The provided siteUrls contain duplicate sites. Remove duplicates.	Ensure SiteUrls must not be the same.
SPE-5150	Invalid Client Id pattern.	Provide the correct client ID.
SPE-5151	Error parsing the field value. Size is over maximum allowed limit.	Ensure the size limit.
SPE-5152	There was a problem while retrieving AD Client ID. AD Client ID should not be empty.	Ensure AD Client Id must be non-empty .
SPE-5153	Invalid AD Client Id pattern.	Provide valid AD Client Id pattern.

Error code	Error message	Suggested resolution
SPE-5154	There was a problem while retrieving AD Client Secret. AD Client Secret should not be empty.	Ensure AD Client Secret is non-empty.
SPE-5155	There can't be more than one site for SharePoin t on-prem app-only authentication.	Ensure that their must be only single site present for SharePoint on-prem app-only authentication.
SPE-5200	There was a problem while connecting to the URL.	Ensure the siteUrl exists.

Connecting SharePoint Server 2019 to Amazon Q Business

Microsoft SharePoint is a collaborative website building service that lets you customize web content and create web pages, web sites, document libraries, and lists. You can connect a SharePoint Server 2019 instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Amazon Q supports Microsoft SharePoint Server (versions 2016, 2019, and Subscription Edition).

Topics

- Known limitations for the Amazon Q Business SharePoint Server 2019 connector
- SharePoint Server 2019 connector overview
- Prerequisites for connecting Amazon Q Business to SharePoint Server 2019
- Connecting Amazon Q Business to SharePoint Server 2019 using the console
- Connecting Amazon Q Business to SharePoint Server 2019 using APIs
- Connecting Amazon Q Business to SharePoint Server 2019 using AWS CloudFormation
- How Amazon Q Business connector crawls SharePoint Server 2019 ACLs
- Amazon Q Business SharePoint Server 2019 data source connector field mappings
- IAM role for Amazon Q Business SharePoint Server 2019 connector

- Understand error codes in the SharePoint Server 2019 connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Amazon Q Business SharePoint Server 2019 connector

The SharePoint Server 2019 connector has the following known limitations:

- The Amazon Q SharePoint connector supports custom field mappings only for the **Files** entity.
- For all SharePoint Server versions, the ACL token must be in lower case. For **Email with Domain from IDP** and **Email ID with Custom Domain** ACL, for example: *`user@sharepoint2019.com`*. For **Domain\User with Domain** ACL, for example: *`sharepoint2013\user`*.
- If an entity name has a `%` character in its name, the connector will skip these files due to API limitations.
- OneNote can only be crawled by the connector using a Tenant ID, and with OAuth 2.0, OAuth 2.0 refresh token, or SharePoint App Only authentication activated for SharePoint Online.
- The connector crawls the first section of a OneNote document using its default name only, even if the document is renamed.
- The connector crawls links in SharePoint 2019 only if **Pages** and **Files** are selected as entities to be crawled in addition to **Links**.
- The connector crawls only list attachments and comments when **List Data** is selected as an entity to be crawled.
- The connector crawls event attachments only when **Events** is also selected as an entity to be crawled.
- To crawl nested groups using **Identity crawler**, you have to activate Local as well as AD Group Crawling.

- To use **Identity Crawler** with SharePoint Server 2019 to crawl nested groups, you have to enable both Local and AD Group Crawling.
- Query responses based on AD Group ACLs are not supported for SharePoint Server 2019. You need to add users and groups directly to your document permissions list.
- When Access Control Lists (ACLs) are enabled, the "Sync only new or modified content" option is not available due to SharePoint Server 2019 API limitations. We recommend using "Full sync" or "New, modified, or deleted content sync" modes instead, or disable ACLs if you need to use this sync mode.

SharePoint Server 2019 connector overview

The following table gives an overview of the Amazon Q Business SharePoint Server 2019 connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	NTLM, Kerberos, SharePoint App-Only (Client Credentials Flow)
	Authentication credentials	**NTLM** • SharePoint admin username • SharePoint admin password If you're using **Email ID with Domain from IDP** to crawl ACLs, then you also need to add a: • LDAP Server Endpoint • LDAP Search Base • LDAP username • LDAP password **Kerberos** • SharePoint admin username

Category	Feature	Support
		• SharePoint admin password If you're using **Email ID with Domain from IDP** to crawl ACLs, then you also need to add a: • LDAP Server Endpoint • LDAP Search Base • LDAP username • LDAP password **SharePoint App-Only (Client Credentials Flow)** • Tenant ID • SharePoint App-Only client ID • SharePoint App-Only client secret If you're using **Email ID with Domain from IDP** to crawl ACLs, then you also need to add a: • LDAP Server Endpoint • LDAP Search Base • LDAP username • LDAP password
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Integration with Identity Provider (IdP)	Yes. LDAP.
	Identity crawling	Yes

Category	Feature	Support
	VPC	Yes
Crawl features	**Entities**	Yes. The following entities are supported: • Files • Attachments • Link • Pages • Events • List data See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Include/exclude by **Links** • Include/exclude by **Pages** • Include/exclude by **Events** • Include/exclude by file name • Include/exclude by file path • Include/exclude by file type • Include/exclude by **OneNote Section** name • Include/exclude by **OneNote Page** name
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to SharePoint Server 2019

The following page outlines the prerequisites you need to complete before connecting SharePoint Server 2019 to Amazon Q, based on the authentication mode of your choice.

Topics

- Prerequisites for using NTLM authentication
- Prerequisites for using Kerberos authentication
- Prerequisites for using SharePoint App-Only authentication

Prerequisites for using NTLM authentication

If you're using NTLM authentication, make sure you've completed the following steps in SharePoint Server 2019:

- Copied your SharePoint instance URLs. The format for the host URL you enter is *`https://yourdomain.sharepoint.com/sites/mysite`*. Your URL must start with `https` and contain `sharepoint.com`.
- Copied the domain name of your SharePoint instance URL.
- Generated an SSL certificate and uploaded it to an Amazon S3 bucket.
- Noted the username and password that you use to connect to SharePoint.

If you're using Email ID with Domain from IDP to control access to your documents, make sure you've completed the following steps:

- Copied your LDAP Server Endpoint (endpoint of LDAP server including protocol and port number). For example: *`ldap://example.com:389`*.
- Copied your LDAP Search Base (search base of the LDAP user). For example: *`CN=Users,DC=sharepoint,DC=com`*.
- Copied your LDAP username and LDAP password.

If using Email ID with Custom Domain for access control, complete the following step:

- Noted your custom email domain value—for example: *`"amazon.com"`*.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your SharePoint Server 2019 authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Prerequisites for using Kerberos authentication

If you're using Kerberos authentication, make sure you've completed the following steps in SharePoint Server 2019:

- Copied your SharePoint instance URLs. The format for the host URL you enter is *`https://yourdomain.sharepoint.com/sites/mysite`*. Your URL must start with `https` and contain `sharepoint.com`.
- Copied the domain name of your SharePoint instance URL.
- Generated an SSL certificate and uploaded it to an Amazon S3 bucket.
- Noted the username and password that you use to connect to SharePoint.

(Optional) If you're using Email ID with Domain from IDP to control access to your documents, make sure you've completed the following steps:

- Copied your LDAP Server Endpoint (endpoint of LDAP server including protocol and port number). For example: *`ldap://example.com:389`*.
- Copied your LDAP Search Base (search base of the LDAP user). For example: *`CN=Users,DC=sharepoint,DC=com`*.
- Copied your LDAP username and LDAP password.

(Optional) If using Email ID with Custom Domain for access control, complete the following step:

- Noted your custom email domain value—for example: *"amazon.com"*.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your SharePoint Server 2019 authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Prerequisites for using SharePoint App-Only authentication

If you're using SharePoint App-Only authentication, make sure you've completed the following steps in SharePoint Server 2019:

- Copied the SharePoint client ID generated when you registered App Only at Site Level. ClientID format is ClientID@TenantId. For example, *ffa956f3-8f89-44e7-b0e4-49670756342c@888d0b57-69f1-4fb8-957f-e1f0bedf82fe*.
- Copied the SharePoint client secret generated when you registered App Only at Site Level.

> **Important**
>
> **Note:** Because client IDs and client secrets are generated for single sites only when you register SharePoint Server for App Only authentication, only one site URL is supported for SharePoint App Only authentication.

- Noted the Tenant ID of your SharePoint account.
- Noted your **LDAP Server Endpoint**, **LDAP Search Base**, **LDAP username**, and **LDAP password**.

> **Note**
>
> SharePoint App-Only Authentication is *not* supported for SharePoint 2013 version.

(Optional) If you're using Email ID with Domain from IDP to control access to your documents, make sure you've completed the following steps:

- Copied your LDAP Server Endpoint (endpoint of LDAP server including protocol and port number). For example: `ldap://example.com:389`.
- Copied your LDAP Search Base (search base of the LDAP user). For example: `CN=Users,DC=sharepoint,DC=com`.
- Copied your LDAP username and LDAP password.

(Optional) If using Email ID with Custom Domain for access control, complete the following step:

- Noted your custom email domain value—for example: `"amazon.com"`.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.

- Stored your SharePoint Server 2019 authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to SharePoint Server 2019 using the console

The following procedure outlines how to connect Amazon Q Business to SharePoint Server 2019 using the AWS Management Console.

Connecting Amazon Q to SharePoint Server 2019

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **SharePoint** data source to your Amazon Q application.
5. Then, on the **SharePoint Server 2019** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

   > **Note**
   >
   > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, enter the following information:

a. In **Source**, for **Hosting Method** – Choose **SharePoint Server**.

b. **Choose SharePoint Version** – Choose **SharePoint 2019**.

c. **Site URLs specific to your SharePoint repository** – Enter the SharePoint host URLs. The format for the host URLs you enter is *`https://yourcompany/sites/mysite`*. The URL must start with `https` protocol. Separate URLs with a new line. You can add up to 100 URLs.

d. **Domain** – Enter the SharePoint domain.

e. **SSL certificate location** – Enter the Amazon S3 path to your SSL certificate file.

8. For **Web proxy – *optional*** – Enter the host name (without the `http://` or `https://` protocol), and the port number used by the host URL transport protocol. The numeric value of the port number must be between 0 and 65535.

9. For **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. You can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details. For SharePoint Server, you can choose from the following ACL options:

   a. **Email ID with Domain from IDP** – Access control is based on email IDs that are extracted from email domains fetched from the underlying identity provider (IdP). You provide the IdP connection details in your Secrets Manager secret during **Authentication**.

   b. **Email ID with Custom Domain** – Access control is based on email IDs. Provide the email domain value. For example, *`"amazon.com"`*. The email domain is used to construct the email ID for access control. You must enter your email domain using **Add Email Domain**.

   See Authorization for more details.

10. For **Authentication**, choose between **SharePoint App-Only authentication**, **NTLM authentication**, and **Kerberos authentication**, based on your use case.

    a. Enter the following information for both **NTLM authentication** and **Kerberos authentication**:

       For **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your SharePoint authentication credentials. If you choose to create a secret,

an AWS Secrets Manager secret window opens. Enter the following information in the window:

- **Secret name** – A name for your secret.
- **Username** – Username for your SharePoint account.
- **Password** – Password for your SharePoint account.

If using **Email ID with Domain from IDP**, also enter your:

- **LDAP Server Endpoint** – Endpoint of LDAP server, including protocol and port number. For example: *ldap://example.com:389*.
- **LDAP Search Base** – Search base of LDAP user. For example: *CN=Users,DC=sharepoint,DC=com*.
- **LDAP username** – Your LDAP username.
- **LDAP Password** – Your LDAP password.

b. Enter the following information for **SharePoint App-Only authentication**:

For **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your SharePoint authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens. Enter the following information in the window:

- **Secret name** – A name for your secret.
- **Client ID** – The SharePoint client ID that you generated when you registered App Only at Site Level. The ClientID format is ClientID@TenantId. For example, *ffa956f3-8f89-44e7-b0e4-49670756342c@888d0b57-69f1-4fb8-957f-e1f0bedf82fe*.
- **SharePoint client secret** – The SharePoint client secret generated when your register for App Only at Site Level.

  Note: Because client IDs and client secrets are generated for single sites only when you register SharePoint Server for App Only authentication, only one site URL is supported for SharePoint App Only authentication.

If using **Email ID with Domain from IDP**, also enter your:

- **LDAP Server Endpoint** – Endpoint of LDAP server, including protocol and port number. For example: *ldap://example.com:389*.
- **LDAP Search Base** – Search base of LDAP user. For example: *CN=Users,DC=sharepoint,DC=com*.
- **LDAP username** – Your LDAP user name.
- **LDAP Password** – Your LDAP password.

11. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

12. **Identity crawler** – Amazon Q crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. Only **Local Group Members** will be crawled by **Identity crawler**. For more information, see Identity crawler.

13. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.

14. In **Sync scope**, choose from the following options :

    a. **Select entities** – Choose the entities that you want to crawl. You can select to crawl **All** entities or any combination of **Files**, **Attachments**, **Links**, **Pages**, **Events** and **List Data**.

b. In **Additional configuration – *optional***, for **Entity regex patterns** – Add regular expression patterns for **Links**, **Pages**, and **Events** to include specific entities instead of syncing all your documents.

c. **Regex patterns** – Add regular expression patterns to include or exclude files by **File path**, **File name**, **File type**, **OneNote section name**, and **OneNote page name** instead of syncing all your documents. You can add up to 100 patterns.

> **Note**
>
> Any valid regex pattern is supported. For example, if you use the regex `^QBusiness*`, any content starting with the word `QBusiness` followed by any number of characters will be filtered (`QBusiness_doc1` or `QBusiness`, but not `doc1_QBusiness`).

d. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

To extract audio transcriptions and video content, enable processing for the following file types:

e. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

15. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

- **Full sync** – Sync all content regardless of the previous sync status.
- **New or modified content sync** – Sync only new and modified documents.
- **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

For more details, see Sync mode.

16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
18. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages,

including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to SharePoint Server 2019 using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- SharePoint Server 2019 configuration properties
- SharePoint Server 2019 JSON schema
- SharePoint Server 2019 JSON schema example

SharePoint Server 2019 configuration properties

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-properties.	Yes

Configuration	Description	Type	Required
		• siteUrls • domain • repository AdditionalProperties • tenantId	
tenantId	The tenant id of your SharePoint account.	string OAuth2 series required	Yes
domain	The domain of your SharePoint account.	string	Yes
siteUrls	The host URLs of your SharePoint account.	array (string) Specify the URL in the pattern https://*	Yes
repository AdditionalProperties	Additional properties to connect with your repository endpoint.	object This property has the following sub-properties. • version • authType • onPremVersion	Yes
authType	The type of authentication you are using: NTLM, Kerberos, or OAuth2App .	string	Yes

Configuration	Description	Type	Required
`version`	The SharePoint version you are using: `Sever`.	`string (Server)`	Yes
`onPremVersion`	The SharePoint version that you are using.	`string` Valid values are (empty), `2013`, `2016`, `2019`, and `SubscriptionEdition` .	Yes
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties. • `event` • `page` • `file` • `link` • `attachment` • `comment`	Yes

Configuration	Description	Type	Required
• event • page • file • link • attachment • comment	A list of objects that map the attributes or field names of your SharePoint Server 2019 pages and assets to Amazon Q index field names.	object These properties have the following sub-properties. • indexFieldName • indexFieldType • dataSourceFieldName • dateFieldFormat	No
indexFieldName	The field name of your SharePoint Server 2019 events, pages, files, links, attachments, or comments.	string	Yes
indexFieldType	The field type of your SharePoint Server 2019 events, pages, files, links, attachments, or comments.	string The allowed values are STRING, STRING_LIST , and DATE.	Yes
dataSourceFieldName	The data source field name of your SharePoint Server 2019 events, pages, files, links, attachments, or comments.	string	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The date format of your SharePoint Server 2019 events, pages, files, links, attachments, or comments.	`string` Specify the date format in the form `yyyy-MM-dd"T"HH:mm:ss"Z"`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties: • crawlAcl • crawlFiles • crawlPages • crawlEvents • crawlComments • crawlLinks • crawlAttachments • crawlListData • isCrawlLocalGroupMapping • isCrawlAdGroupMapping • aclConfiguration • emailDomain • maxFileSizeInMegaBytes • eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx	Yes

Configuration	Description	Type	Required
		• inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotePageNamePatterns	

Configuration	Description	Type	Required
		• `proxyHost` • `proxyPort`	

Configuration	Description	Type	Required
• eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePa	A list of regular expression patterns to include/exclude specific files in your SharePoint data source. Files that match the patterns are included in the index. File that don&t match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn&t included in the index.	array (string)	No

Configuration	Description	Type	Required
geNamePat terns • exclusion OneNotePa geNamePat terns • emailDomain			
aclConfig uration	Specifes how your ACL is configured.	string> Valid values are ACLWithLD APEmailFm t , ACLWithMa nualEmailFmt , or ACLWithUs ernameFmt .	No
proxyHost	The host where the web proxy is required. The host name should be without protocol (http:// or https://).	string	Yes
proxyPort	Port used by the host URL transport protocol. The port number should be a numeric value between 0 and 65535.	string	Yes

Configuration	Description	Type	Required
• crawlAcl • crawlFiles • crawlPages • crawlEvents • crawlComments • crawlLinks • crawlAttachments • crawlListData • isCrawlLocalGroupMapping • isCrawlAdGroupMapping	Input TRUE to index.	boolean	No
maxFileSizeInMegaBytes	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	string	No

Configuration	Description	Type	Required
`sslCertificatePath`	Configuration information to access the SSL certificate stored in your Amazon S3 bucket.	`object` This property has the following sub-properties. • `bucket` • `key`	No
`bucket`	The name of the Amazon S3 bucket that stores your Microsoft Entra ID (formerly Azure AD) self-signed X.509 certificate.	`string`	Yes
`key`	The name of the SSL certificate stored in your Amazon S3 bucket.	`string`	Yes
`type`	We recommend that you use `SHAREPOINTV2` as your data source type.	`string` Valid values are `SHAREPOINTV2` and `SHAREPOINT`.	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. See Identity crawler for more information.	`boolean`	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index	Yes

Configuration	Description	Type	Required
secretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your SharePoint. If you use OAuth2App authentication, provide the client ID, client secret, LDAP URL, LDAP base DN, LDAP user name, and LDAP password. If you use NTLM or Kerberos authentication, provide the user name, password, LDAP URL, Base DN, LDAP user, and LDAP password.	string The minimum length is 20 and the maximum length is 2,048 characters. If you use Sharepoint App-Only authentication (authType should be 0Auth2App authentication) the secret must contain a JSON structure with the following keys: { "clientId": "*client ID*", "clientSecret": " *client secret*", "ldapUrl": "*LDAP URL*", "ldbaseDn": "*LDAP base DN*", "ldapUser": " *LDAP user name*", "ldapPassword": " *LDAP password*" } If you use NTLM authentication or Kerberos authentic	Yes

Configuration	Description	Type	Required
		ation, the secret must contain a JSON structure with the following keys: `{ "userName": "SharePoint account user name", "password": " SharePoint account password", "ldapUrl": "LDAP URL", "baseDn": "LDAP base DN", "ldapUser": " LDAP user name", "ldapPassword": " LDAP password" }`	
`version`	The version of this template that&s currently supported.	`string`	No

SharePoint Server 2019 JSON schema

The following is the SharePoint Server 2019 JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
```

```
      "enum": ["SHAREPOINTV2", "SHAREPOINT"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "sslCertificatePath": {
      "type": "object",
      "properties": {
        "bucket": {
          "type": "string",
          "pattern": "^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$",
          "minLength": 3,
          "maxLength": 63
        },
        "key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 10240
        }
      },
      "required": ["bucket", "key"]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
```

```
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            },
            "domain": {
              "type": "string"
            },
            "siteUrls": {
              "type": "array",
              "items": {
                "type": "string",
                "pattern": "https://.*"
              }
            },
            "repositoryAdditionalProperties": {
              "type": "object",
              "properties": {
                "authType": {
                  "type": "string",
                  "enum": ["OAuth2App", "NTLM", "Kerberos"]
                },
                "version": {
                  "type": "string",
                  "enum": ["Server"]
                },
                "onPremVersion": {
                  "type": "string",
                  "enum": ["", "2013", "2016", "2019", "SubscriptionEdition"]
                },
                "enableDeletionProtection": {
                  "anyOf": [
                    {
                      "type": "boolean"
                    },
                    {
                      "type": "string",
                      "enum": ["true", "false"]
                    }
                  ],
                  "default": false
```

```
              },
              "deletionProtectionThreshold": {
                "type": "string",
                "default": "15"
              }
            },
            "required": ["authType", "version"]
          }
        },
        "required": ["siteUrls", "domain", "repositoryAdditionalProperties"]
      }
    },
    "required": ["repositoryEndpointMetadata"]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "event": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
```

```
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "page": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "file": {
```

```
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "link": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "attachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
```

```
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "comment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
```

```
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "eventTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "pageTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "linkTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionFilePath": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionFilePath": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionFileTypePatterns": {
        "type": "array",
```

```
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionOneNoteSectionNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionOneNoteSectionNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionOneNotePageNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionOneNotePageNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
```

```
          }
        },
        "crawlFiles": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlPages": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlEvents": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlComments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
```

```
          ]
        },
        "crawlLinks": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAttachments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlListData": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
```

```
          ]
        },
        "aclConfiguration": {
          "type": "string",
          "enum": [
            "ACLWithLDAPEmailFmt",
            "ACLWithManualEmailFmt",
            "ACLWithUsernameFmt"
          ]
        },
        "emailDomain": {
          "type": "string"
        },
        "isCrawlLocalGroupMapping": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlAdGroupMapping": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "proxyHost": {
          "type": "string"
        },
        "proxyPort": {
          "type": "string"
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        }
```

```
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "type",
    "secretArn",
    "syncMode",
    "enableIdentityCrawler",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

SharePoint Server 2019 JSON schema example

The following is the SharePoint Server 2019 JSON schema example:

```
{

  "type": "SHAREPOINTV2",

  "syncMode": "FULL_CRAWL",

  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-sharepoint-
secret",

  "enableIdentityCrawler": "true",

  "sslCertificatePath": {

    "bucket": "my-sharepoint-bucket",

    "key": "ssl/cert.pem"
```

```
  },
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "tenantId": "1234567a-890b-1234-567c-123456789012",
      "domain": "mycompany.sharepoint.com",
      "siteUrls": [
        "https://mycompany.sharepoint.com/sites/TeamSite"
      ],
      "repositoryAdditionalProperties": {
        "authType": "OAuth2",
        "version": "Server",
        "onPremVersion": "2019",
        "enableDeletionProtection": "false",
        "deletionProtectionThreshold": "15"
      }
    }
  },
  "repositoryConfigurations": {
    "event": {
      "fieldMappings": [
        {
          "indexFieldName": "event_id",
          "indexFieldType": "STRING",
```

```
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    ]
  },
  "page": {
    "fieldMappings": [
      {
        "indexFieldName": "page_id",
        "indexFieldType": "STRING",
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    ]
  },
  "file": {
    "fieldMappings": [
      {
        "indexFieldName": "file_id",
        "indexFieldType": "STRING",
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
```

```
        }
      ]
    },
    "link": {
      "fieldMappings": [
        {
          "indexFieldName": "link_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "attachment": {
      "fieldMappings": [
        {
          "indexFieldName": "attachment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
```

```
    },

    "comment": {

      "fieldMappings": [

        {

          "indexFieldName": "comment_id",

          "indexFieldType": "STRING",

          "dataSourceFieldName": "id",

          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"

        }

      ]

    }

  },

  "additionalProperties": {

    "eventTitleFilterRegEx": [
      "^.*$"
    ],

    "pageTitleFilterRegEx": [
      "^.*$"
    ],

    "linkTitleFilterRegEx": [
      "^.*$"
    ],

    "inclusionFilePath": [
      "documents/"
    ],

    "exclusionFilePath": [
      "drafts/"
```

```
    ],

    "inclusionFileTypePatterns": [
      "*.pdf",
       "*.docx"
    ],

    "exclusionFileTypePatterns": [
      "*.tmp"
    ],

    "inclusionFileNamePatterns": [
      "*report*"
    ],

    "exclusionFileNamePatterns": [
      "*draft*"
    ],

    "inclusionOneNoteSectionNamePatterns": [
      "*"
    ],

    "exclusionOneNoteSectionNamePatterns": [
      "archived"
    ],

    "inclusionOneNotePageNamePatterns": [
      "*"
    ],

    "exclusionOneNotePageNamePatterns": [
      "test"
    ],

    "crawlFiles": "true",

    "crawlPages": "true",

    "crawlEvents": "true",

    "crawlComments": "true",

    "crawlLinks": "true",
```

```
    "crawlAttachments": "true",
    "crawlListData": "false",
    "crawlAcl": "true",
    "aclConfiguration": "ACLWithUsernameFmt",
    "emailDomain": "mycompany.com",
    "isCrawlLocalGroupMapping": "false",
    "isCrawlAdGroupMapping": "true",
    "proxyHost": "proxy.mycompany.com",
    "proxyPort": "8080",
    "maxFileSizeInMegaBytes": "50"
  },
  "version": "1.0.0"
}
```

Connecting Amazon Q Business to SharePoint Server 2019 using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- SharePoint Server 2019 configuration properties
- SharePoint Server 2019 JSON schema for using the configuration property with AWS CloudFormation

- SharePoint Server 2019 YAML schema for using the configuration property with AWS CloudFormation

SharePoint Server 2019 configuration properties

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-properties. • `siteUrls` • `domain` • `repositoryAdditionalProperties` • `tenantId`	Yes
`tenantId`	The tenant id of your SharePoint account.	`string` OAuth2 series required	Yes
`domain`	The domain of your SharePoint account.	`string`	Yes

Configuration	Description	Type	Required
`siteUrls`	The host URLs of your SharePoint account.	`array (string)` Specify the URL in the pattern `https://*`	Yes
`repositoryAdditionalProperties`	Additional properties to connect with your repository endpoint.	`object` This property has the following sub-properties. • `version` • `authType` • `onPremVersion`	Yes
`authType`	The type of authentication you are using: `NTLM`, `Kerberos`, or `OAuth2App` .	`string`	Yes
`version`	The SharePoint version you are using: `Sever`.	`string (Server)`	Yes
`onPremVersion`	The SharePoint version that you are using.	`string` Valid values are (empty), `2013`, `2016`, `2019`, and `SubscriptionEdition` .	Yes

Configuration	Description	Type	Required
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties. • `event` • `page` • `file` • `link` • `attachment` • `comment`	Yes
• `event` • `page` • `file` • `link` • `attachment` • `comment`	A list of objects that map the attributes or field names of your SharePoint Server 2019 pages and assets to Amazon Q index field names.	`object` These properties have the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName` • `dateFieldFormat`	No
`indexFieldName`	The field name of your SharePoint Server 2019 events, pages, files, links, attachments, or comments.	`string`	Yes

Configuration	Description	Type	Required
`indexFieldType`	The field type of your SharePoint Server 2019 events, pages, files, links, attachments, or comments.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes
`dataSourceFieldName`	The data source field name of your SharePoint Server 2019 events, pages, files, links, attachments, or comments.	`string`	Yes
`dateFieldFormat`	The date format of your SharePoint Server 2019 events, pages, files, links, attachments, or comments.	`string` Specify the date format in the form `yyyy-MM-dd"T"HH:mm:ss"Z"`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties: • crawlAcl • crawlFiles • crawlPages • crawlEvents • crawlComments • crawlLinks • crawlAttachments • crawlListData • isCrawlLocalGroupMapping • isCrawlAdGroupMapping • aclConfiguration • emailDomain • maxFileSizeInMegaBytes • eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx	Yes

Configuration	Description	Type	Required
		• inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotePageNamePatterns	

Configuration	Description	Type	Required
		• `proxyHost` • `proxyPort`	

Configuration	Description	Type	Required
• eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePa	A list of regular expression patterns to include/exclude specific files in your SharePoint data source. Files that match the patterns are included in the index. File that don&t match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn&t included in the index.	array (string)	No

Configuration	Description	Type	Required
geNamePat terns • exclusion OneNotePa geNamePat terns • emailDomain			
aclConfig uration	Specifes how your ACL is configured.	string> Valid values are ACLWithLD APEmailFm t , ACLWithMa nualEmailFmt , or ACLWithUs ernameFmt .	No
proxyHost	The host where the web proxy is required. The host name should be without protocol (http:// or https://).	string	Yes
proxyPort	Port used by the host URL transport protocol. The port number should be a numeric value between 0 and 65535.	string	Yes

Configuration	Description	Type	Required
• crawlAcl • crawlFiles • crawlPages • crawlEvents • crawlComments • crawlLinks • crawlAttachments • crawlListData • isCrawlLocalGroupMapping • isCrawlAdGroupMapping	Input TRUE to index.	boolean	No
maxFileSizeInMegaBytes	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	string	No

Configuration	Description	Type	Required
`sslCertificatePath`	Configuration information to access the SSL certificate stored in your Amazon S3 bucket.	`object` This property has the following sub-properties. • `bucket` • `key`	No
`bucket`	The name of the Amazon S3 bucket that stores your Microsoft Entra ID (formerly Azure AD) self-signed X.509 certificate.	`string`	Yes
`key`	The name of the SSL certificate stored in your Amazon S3 bucket.	`string`	Yes
`type`	We recommend that you use `SHAREPOINTV2` as your data source type.	`string` Valid values are `SHAREPOINTV2` and `SHAREPOINT`.	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. See Identity crawler for more information.	`boolean`	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index	Yes

Configuration	Description	Type	Required
secretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your SharePoint. If you use OAuth2App authentication, provide the client ID, client secret, LDAP URL, LDAP base DN, LDAP user name, and LDAP password. If you use NTLM or Kerberos authentication, provide the user name, password, LDAP URL, Base DN, LDAP user, and LDAP password.	string The minimum length is 20 and the maximum length is 2,048 characters. If you use Sharepoint App-Only authentication (authType should be 0Auth2App authentication) the secret must contain a JSON structure with the following keys: { "clientId": "*client ID*", "clientSecret": " *client secret*", "ldapUrl": "*LDAP URL*", "ldbaseDn": "*LDAP base DN*", "ldapUser": " *LDAP user name*", "ldapPassword": " *LDAP password*" } If you use NTLM authentication or Kerberos authentic	Yes

Configuration	Description	Type	Required
		ation, the secret must contain a JSON structure with the following keys: `{ "userName": "SharePoint account user name", "password": " SharePoint account password", "ldapUrl": "LDAP URL", "baseDn": "LDAP base DN", "ldapUser": " LDAP user name", "ldapPassword": " LDAP password" }`	
`version`	The version of this template that&s currently supported.	`string`	No

SharePoint Server 2019 JSON schema for using the configuration property with AWS CloudFormation

The following is the SharePoint Server 2019 JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- SharePoint Server 2019 JSON schema for using the configuration property with AWS CloudFormation
- SharePoint Server 2019 JSON schema example for using the configuration property with AWS CloudFormation

SharePoint Server 2019 JSON schema for using the configuration property with AWS CloudFormation

The following is the SharePoint Server 2019 JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["SHAREPOINTV2", "SHAREPOINT"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "sslCertificatePath": {
      "type": "object",
      "properties": {
        "bucket": {
```

```
          "type": "string",
          "pattern": "^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$",
          "minLength": 3,
          "maxLength": 63
        },
        "key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 10240
        }
      },
      "required": ["bucket", "key"]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            },
            "domain": {
              "type": "string"
            },
            "siteUrls": {
              "type": "array",
              "items": {
                "type": "string",
                "pattern": "https://.*"
              }
            },
            "repositoryAdditionalProperties": {
              "type": "object",
              "properties": {
                "authType": {
                  "type": "string",
                  "enum": ["OAuth2App", "NTLM", "Kerberos"]
                },
                "version": {
```

```
                "type": "string",
                "enum": ["Server"]
              },
              "onPremVersion": {
                "type": "string",
                "enum": ["", "2013", "2016", "2019", "SubscriptionEdition"]
              },
              "enableDeletionProtection": {
                "anyOf": [
                  {
                    "type": "boolean"
                  },
                  {
                    "type": "string",
                    "enum": ["true", "false"]
                  }
                ],
                "default": false
              },
              "deletionProtectionThreshold": {
                "type": "string",
                "default": "15"
              }
            },
            "required": ["authType", "version"]
          }
        },
        "required": ["siteUrls", "domain", "repositoryAdditionalProperties"]
      }
    },
    "required": ["repositoryEndpointMetadata"]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "event": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
```

```
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "page": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
```

```
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "file": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
```

```
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "link": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "attachment": {
```

```
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "comment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "eventTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "pageTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "linkTitleFilterRegEx": {
        "type": "array",
```

```
          "items": {
            "type": "string"
          }
        },
        "inclusionFilePath": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFilePath": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionOneNoteSectionNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
```

```
        }
      },
      "exclusionOneNoteSectionNamePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionOneNotePageNamePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionOneNotePageNamePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "crawlFiles": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlPages": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlEvents": {
        "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlComments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlLinks": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAttachments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlListData": {
          "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "aclConfiguration": {
          "type": "string",
          "enum": [
            "ACLWithLDAPEmailFmt",
            "ACLWithManualEmailFmt",
            "ACLWithUsernameFmt"
          ]
        },
        "emailDomain": {
          "type": "string"
        },
        "isCrawlLocalGroupMapping": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlAdGroupMapping": {
          "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "proxyHost": {
          "type": "string"
        },
        "proxyPort": {
          "type": "string"
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "type",
    "secretArn",
    "syncMode",
    "enableIdentityCrawler",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

SharePoint Server 2019 JSON schema example for using the configuration property with AWS CloudFormation

The following is the SharePoint Server 2019 JSON schema example for the configuration property for CloudFormation

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation SHAREPOINT Data Source Template",
  "Resources": {
    "DataSourceSharePoint": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MySharePointDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "SHAREPOINTV2",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-
sharepoint-secret",
          "enableIdentityCrawler": "true",
          "sslCertificatePath": {
            "bucket": "my-sharepoint-bucket",
```

```
            "key": "ssl/cert.pem"

          },

          "connectionConfiguration": {

            "repositoryEndpointMetadata": {

              "tenantId": "1234567a-890b-1234-567c-123456789012",

              "domain": "mycompany.sharepoint.com",

              "siteUrls": [
                "https://mycompany.sharepoint.com/sites/TeamSite"
              ],

              "repositoryAdditionalProperties": {

                "authType": "OAuth2",

                "version": "Server",

                "onPremVersion": "2019",

                "enableDeletionProtection": "false",

                "deletionProtectionThreshold": "15"

              }

            }

          },

          "repositoryConfigurations": {

            "event": {

              "fieldMappings": [

                {

                  "indexFieldName": "event_id",
```

```
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "page": {
        "fieldMappings": [
          {
            "indexFieldName": "page_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "file": {
        "fieldMappings": [
          {
            "indexFieldName": "file_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
```

```
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "link": {
        "fieldMappings": [
          {
            "indexFieldName": "link_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "attachment": {
        "fieldMappings": [
          {
            "indexFieldName": "attachment_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
```

```
        ]

      },

      "comment": {

        "fieldMappings": [

          {

            "indexFieldName": "comment_id",

            "indexFieldType": "STRING",

            "dataSourceFieldName": "id",

            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"

          }

        ]

      }

    },

    "additionalProperties": {

      "eventTitleFilterRegEx": [
        "^.*$"
      ],

      "pageTitleFilterRegEx": [
        "^.*$"
      ],

      "linkTitleFilterRegEx": [
        "^.*$"
      ],

      "inclusionFilePath": [
        "documents/"
      ],
```

```
            "exclusionFilePath": [
              "drafts/"
            ],

            "inclusionFileTypePatterns": [
              "*.pdf",
               "*.docx"
            ],

            "exclusionFileTypePatterns": [
              "*.tmp"
            ],

            "inclusionFileNamePatterns": [
              "*report*"
            ],

            "exclusionFileNamePatterns": [
              "*draft*"
            ],

            "inclusionOneNoteSectionNamePatterns": [
              "*"
            ],

            "exclusionOneNoteSectionNamePatterns": [
              "archived"
            ],

            "inclusionOneNotePageNamePatterns": [
              "*"
            ],

            "exclusionOneNotePageNamePatterns": [
              "test"
            ],

            "crawlFiles": "true",

            "crawlPages": "true",

            "crawlEvents": "true",

            "crawlComments": "true",
```

```
            "crawlLinks": "true",
            "crawlAttachments": "true",
            "crawlListData": "false",
            "crawlAcl": "true",
            "aclConfiguration": "ACLWithUsernameFmt",
            "emailDomain": "mycompany.com",
            "isCrawlLocalGroupMapping": "false",
            "isCrawlAdGroupMapping": "true",
            "proxyHost": "proxy.mycompany.com",
            "proxyPort": "8080",
            "maxFileSizeInMegaBytes": "50"
          }
        }
      }
    }
  }
}
```

SharePoint Server 2019 YAML schema for using the configuration property with AWS CloudFormation

The following is the SharePoint Server 2019 YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- SharePoint Server 2019 YAML schema for using the configuration property with AWS CloudFormation
- SharePoint Server 2019 YAML schema example for using the configuration property with AWS CloudFormation

SharePoint Server 2019 YAML schema for using the configuration property with AWS CloudFormation

The following is the SharePoint Server 2019 YAML schema for the configuration property for CloudFormation.

```
type: object
properties:
  type:
    type: string
    enum:
      - SHAREPOINTV2
      - SHAREPOINT
  syncMode:
    type: string
    enum:
      - FULL_CRAWL
      - FORCED_FULL_CRAWL
      - CHANGE_LOG
  secretArn:
    type: string
    minLength: 20
    maxLength: 2048
  enableIdentityCrawler:
    anyOf:
      - type: boolean
      - type: string
        enum:
          - true
          - false
  sslCertificatePath:
    type: object
    properties:
      bucket:
        type: string
        pattern: '^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$'
        minLength: 3
```

```
        maxLength: 63
      key:
        type: string
        minLength: 1
        maxLength: 10240
    required:
      - bucket
      - key
  connectionConfiguration:
    type: object
    properties:
      repositoryEndpointMetadata:
        type: object
        properties:
          tenantId:
            type: string
            pattern: "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$"
            minLength: 36
            maxLength: 36
          domain:
            type: string
          siteUrls:
            type: array
            items:
              type: string
              pattern: "https://.*"
          repositoryAdditionalProperties:
            type: object
            properties:
              authType:
                type: string
                enum:
                  - OAuth2App
                  - NTLM
                  - Kerberos
              version:
                type: string
                enum:
                  - Server
              onPremVersion:
                type: string
                enum:
                  - ""
                  - "2013"
```

```
                - "2016"
                - "2019"
                - SubscriptionEdition
            enableDeletionProtection:
              anyOf:
                - type: boolean
                - type: string
                  enum:
                    - true
                    - false
              default: false
            deletionProtectionThreshold:
              type: string
              default: "15"
          required:
            - authType
            - version
      required:
        - siteUrls
        - domain
        - repositoryAdditionalProperties
  required:
    - repositoryEndpointMetadata
repositoryConfigurations:
  type: object
  properties:
    event:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
```

```
            dateFieldFormat:
              type: string
              pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
          required:
            - indexFieldName
            - indexFieldType
            - dataSourceFieldName
      required:
        - fieldMappings
    page:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - DATE
                  - LONG
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    file:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
```

```
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - DATE
                  - LONG
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
        required:
          - fieldMappings
      link:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
```

```
        required:
          - fieldMappings
      attachment:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      comment:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
```

```
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
  required: []
additionalProperties:
  type: object
  properties:
    eventTitleFilterRegEx:
      type: array
      items:
        type: string
    pageTitleFilterRegEx:
      type: array
      items:
        type: string
    linkTitleFilterRegEx:
      type: array
      items:
        type: string
    inclusionFilePath:
      type: array
      items:
        type: string
    exclusionFilePath:
      type: array
      items:
        type: string
    inclusionFileTypePatterns:
      type: array
      items:
        type: string
    exclusionFileTypePatterns:
      type: array
      items:
        type: string
```

```
      inclusionFileNamePatterns:
        type: array
        items:
          type: string
      exclusionFileNamePatterns:
        type: array
        items:
          type: string
      inclusionOneNoteSectionNamePatterns:
        type: array
        items:
          type: string
      exclusionOneNoteSectionNamePatterns:
        type: array
        items:
          type: string
      inclusionOneNotePageNamePatterns:
        type: array
        items:
          type: string
      exclusionOneNotePageNamePatterns:
        type: array
        items:
          type: string
      crawlFiles:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlPages:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlEvents:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
```

```
            - false
      crawlComments:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlLinks:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlAttachments:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlListData:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlAcl:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      aclConfiguration:
        type: string
        enum:
          - ACLWithLDAPEmailFmt
          - ACLWithManualEmailFmt
          - ACLWithUsernameFmt
      emailDomain:
        type: string
```

```
      isCrawlLocalGroupMapping:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      isCrawlAdGroupMapping:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      proxyHost:
        type: string
      proxyPort:
        type: string
      maxFileSizeInMegaBytes:
        type: string
    required: []
  version:
    type: string
    anyOf:
      - pattern: 1.0.0
required:
  - type
  - secretArn
  - syncMode
  - enableIdentityCrawler
  - connectionConfiguration
  - repositoryConfigurations
  - additionalProperties
```

SharePoint Server 2019 YAML schema example for using the configuration property with AWS CloudFormation

The following is the SharePoint Server 2019 YAML example for the Configuration property for CloudFormation:

```
{
```

```
  "type": "SHAREPOINTV2",

  "syncMode": "FULL_CRAWL",

  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-sharepoint-
secret",

  "enableIdentityCrawler": "true",

  "sslCertificatePath": {

    "bucket": "my-sharepoint-bucket",

    "key": "ssl/cert.pem"

  },

  "connectionConfiguration": {

    "repositoryEndpointMetadata": {

      "tenantId": "1234567a-890b-1234-567c-123456789012",

      "domain": "mycompany.sharepoint.com",

      "siteUrls": [
        "https://mycompany.sharepoint.com/sites/TeamSite"
      ],

      "repositoryAdditionalProperties": {

        "authType": "OAuth2",

        "version": "Server",

        "onPremVersion": "2019",

        "enableDeletionProtection": "false",

        "deletionProtectionThreshold": "15"

      }

    }
```

```
},
"repositoryConfigurations": {
  "event": {
    "fieldMappings": [
      {
        "indexFieldName": "event_id",
        "indexFieldType": "STRING",
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    ]
  },
  "page": {
    "fieldMappings": [
      {
        "indexFieldName": "page_id",
        "indexFieldType": "STRING",
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    ]
  },
```

```
    "file": {
      "fieldMappings": [
        {
          "indexFieldName": "file_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "link": {
      "fieldMappings": [
        {
          "indexFieldName": "link_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "attachment": {
      "fieldMappings": [
```

```
        {
          "indexFieldName": "attachment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "comment": {
      "fieldMappings": [
        {
          "indexFieldName": "comment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    }
  },
  "additionalProperties": {
    "eventTitleFilterRegEx": [
      "^.*$"
    ],
```

```
"pageTitleFilterRegEx": [
  "^.*$"
],

"linkTitleFilterRegEx": [
  "^.*$"
],

"inclusionFilePath": [
  "documents/"
],

"exclusionFilePath": [
  "drafts/"
],

"inclusionFileTypePatterns": [
  "*.pdf",
   "*.docx"
],

"exclusionFileTypePatterns": [
  "*.tmp"
],

"inclusionFileNamePatterns": [
  "*report*"
],

"exclusionFileNamePatterns": [
  "*draft*"
],

"inclusionOneNoteSectionNamePatterns": [
  "*"
],

"exclusionOneNoteSectionNamePatterns": [
  "archived"
],

"inclusionOneNotePageNamePatterns": [
  "*"
```

```
    ],

    "exclusionOneNotePageNamePatterns": [
      "test"
    ],

    "crawlFiles": "true",

    "crawlPages": "true",

    "crawlEvents": "true",

    "crawlComments": "true",

    "crawlLinks": "true",

    "crawlAttachments": "true",

    "crawlListData": "false",

    "crawlAcl": "true",

    "aclConfiguration": "ACLWithUsernameFmt",

    "emailDomain": "mycompany.com",

    "isCrawlLocalGroupMapping": "false",

    "isCrawlAdGroupMapping": "true",

    "proxyHost": "proxy.mycompany.com",

    "proxyPort": "8080",

    "maxFileSizeInMegaBytes": "50"

  },

  "version": "1.0.0"

}
```

How Amazon Q Business connector crawls SharePoint Server 2019 ACLs

When you connect an SharePoint Server 2019 data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your SharePoint Server 2019 instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

To filter using a username, use the **User principal name** from your Azure portal. For example, johnstiles@kendra.onmicrosoft.com.

When you use a SharePoint group for user context filtering, calculate the group ID as follows:

For local groups

1. Get the site name. For example, `https://host.onmicrosoft.com/sites/siteName`.
2. Take the SHA256 hash of the site name. For example, `430a6b90503eef95c89295c8999c7981`.
3. Create the group ID by concatenating the SHA256 hash with a vertical bar (|) and the group name. For example, if the group name is "local group name", the group ID is the following:

   `"430a6b90503eef95c89295c8999c7981 | localGroupName"` (with a space before and after the vertical bar).

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Amazon Q Business SharePoint Server 2019 data source connector field mappings

To help you structure data for retrieval and chat filtering, Amazon Q Business crawls data source document attributes or metadata and maps them to fields in your Amazon Q index.

Amazon Q has reserved fields that it uses when querying your application. When possible, Amazon Q automatically maps these built-in fields to attributes in your data source. If a built-in field doesn't have a default mapping, or if you want to map additional index fields, use the custom field mappings to specify how a data source attribute maps to your Amazon Q application. You create

field mappings by editing your data source after your application environment and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Sharepoint connector supports the following entities and the associated reserved and custom attributes.

> **Important**
>
> If you map any SharePoint Server 2019 field to Amazon Q document title and document body fields, Amazon Q will generate responses from data in the document title and body.

> **Note**
>
> You can map any Sharepoint field to the document title or document body Amazon Q reserved/default index fields.

Supported entities and field mappings

- Files
- Events
- Pages
- Links
- Attachments

Files

Sharepoint field name	Index field name	Description	Data type
title	_document_title	Default	String
lastModifiedDateTime	_last_updated_at	Default	Date
sourceUri	_source_uri	Default	String
checkInComment	sp_checkInComment	Custom	String
createdAt	_created_at	Default	Date
size	sp_sizeLong	Custom	Long (numeric)
majorVersion	sp_majorVersion	Custom	String
uiVersionLabel	sp_uiVersionLabel	Custom	String
uniqueId	sp_uniqueId	Custom	String
irmEnabled	sp_irmEnabled	Custom	String
checkOutType	sp_checkOutType	Custom	String
author	_authors	Default	String list
category	_category	Default	String
modifiedBy	sp_modifiedBy	Custom	String
level	sp_level	Custom	String
uiVersion	sp_uiVersion	Custom	String
contentTag	sp_contentTag	Custom	String
eTag	sp_eTag	Custom	String

Sharepoint field name	Index field name	Description	Data type
oneNoteDocument	sp_oneNoteDocument	Custom	String
oneNoteSection	sp_oneNoteSection	Custom	String
oneNotePage	sp_oneNotePage	Custom	String

Events

Sharepoint field name	Index field name	Description	Data type
title	_document_title	Default	String
lastModifiedDateTime	_last_updated_at	Default	Date
sourceUri	_source_uri	Default	String
attachments	sp_hasAttachments	Custom	String
createdDate	_created_at	Default	Date
authorId	sp_authorId	Custom	String
editorId	sp_editorId	Custom	String
location	sp_location	Custom	String
eventDate	sp_eventDate	Custom	Date
eventEndDate	sp_eventEndDate	Custom	Date
ifRecurrence	sp_ifRecurrence	Custom	String
ifAllDayEvent	sp_ifAllDayEvent	Custom	String

Sharepoint field name	Index field name	Description	Data type
category	_category	Default	String
eventCategory	sp_eventcategory	Custom	String

Pages

Sharepoint field name	Index field name	Description	Data type
createdDateTime	_created_at	Default	Date
lastModifiedDateTime	_last_updated_at	Default	Date
title	_document_title	Default	String
sourceUri	_source_uri	Default	String
firstPublishedDate	sp_firstPublishedDate	Custom	Date
authorId	sp_authorId	Custom	String
editorId	sp_editorId	Custom	String
category	_category	Default	String

Links

Sharepoint field name	Index field name	Description	Data type
createdAt	_created_at	Default	Date
lastModifiedDateTime	_last_updated_at	Default	Date

Sharepoint field name	Index field name	Description	Data type
title	_document_title	Default	String
sourceUri	_source_uri	Default	String
fileType	sp_fileType	Custom	String
fileDirPath	sp_fileDirPath	Custom	String
firstPublishedDate	sp_firstPublishedDate	Custom	Date
authorId	sp_authorId	Custom	String
editorId	sp_editorId	Custom	String
category	_category	Default	String
size	sp_sizeLong	Custom	Long (numeric)

Attachments

Sharepoint field name	Index field name	Description	Data type
title	sp__title	Custom	String
parentCreatedDate	_created_at	Default	Date
sourceUri	_source_uri	Default	String
parentModifiedDate	_last_updated_at	Custom	Date
parentListId	sp_parentListId	Custom	String
parentTitle	sp_parentTitle	Custom	String
category	_category	Default	String

IAM role for Amazon Q Business SharePoint Server 2019 connector

> **Note**
>
> **(Optional)** If you use **Azure App-Only authentication**, you also need to add permissions for Amazon Q to access the certificate stored in your Amazon S3 bucket.

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
```

```
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
```

```
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
"qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
"qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the SharePoint Server 2019 connector

The following table provides information about error codes you may see for the Microsoft SharePoint connector and suggested resolutions.

Error code	Error message	Suggested resolution
SPE-5001	Authentication failed. Configuration might contain wrong credentia ls.	Provide valid credentials like username, password or client Id, client secret and tenant Id.
SPE-5002	There was a problem while connecting to Host Url and/or Domain. hostUrl and/or domain values might be incorrect .	Provide valid Host URL or Domain.
SPE-5003	Provided URL is incorrect	Provide correct URL.
SPE-5004	Inet Address validation Failed.	Provide valid Inet Address
SPE-5005	Failed : HTTP protocol violation has occurred.	Try running the connector again.
SPE-5006	Cannot connect to proxy. Check the proxy configurations.	Provide valid Proxy configuration details.
SPE-5007	Proxy port is invalid. Check the proxy port.	Provide valid Proxy port.
SPE-5008	Valid SSL Certificate could not be found for connector.	Provide valid SSL certificate.
SPE-5009	There was a problem while connecting to	Provide valid LDAP configuration details.

Error code	Error message	Suggested resolution
	LDAP. Check LDAP configuration.	
SPE-5100	There was a problem while retrieving repository Id. Repository ID might be empty or null.	Ensure that repository Id must not be null or empty.
SPE-5101	There was a problem while retrieving dataSourceIamRoleArn. Data Source IAM Role ARN might be empty or null.	Ensure that dataSourceIamRoleArn must not be null or empty.
SPE-5102	There was a problem while retrieving repository configurations. Repository configurations might be empty or incorrect.	Provide valid repository configurations.
SPE-5115	There was a problem while retrieving field mapping values for event entity. Field mapping values might be empty or incorrect.	Field mapping values for event entity should be correct or non-empty.
SPE-5116	There was a problem while retrieving field mapping values for file entity. Field mapping values might be empty or incorrect.	Field mapping values for file entity should be correct or non-empty.

Error code	Error message	Suggested resolution
SPE-5117	There was a problem while retrieving field mapping values for page entity. Field mapping values might be empty or incorrect.	Field mapping values for page entity should be correct or non-empty.
SPE-5118	There was a problem while retrieving field mapping values for link entity. Field mapping values might be empty or incorrect.	Field mapping values for link entity should be correct or non-empty.
SPE-5119	There was a problem while retrieving field mapping values for comment entity. Field mapping values might be empty or incorrect.	Field mapping values for comment entity should be correct or non-empty.
SPE-5120	There was a problem while retrieving field mapping values for attachment entity. Field mapping values might be empty or incorrect.	Field mapping values for attachment entity should be correct or non-empty.
SPE-5121	There was a problem while retrieving values for crawl entities. Values might be empty or incorrect. It should be either true or false.	There might be some incorrect value given in any one of the crawling entities like – null, TRUE or any dummy string. Ensure the value must be non-empty and either true or false.

Error code	Error message	Suggested resolution
SPE-5122	There was a problem while retrieving domain. Domain might be empty or null.	Provide Client Id.
SPE-5123	There was a problem while retrieving version. Version might be empty or null.	Provide valid version and it should not be null.
SPE-5124	There was a problem while retrieving authType. Auth-Type might be empty or null.	Ensure AUTH Type in configuration must be not null.
SPE-5125	There was a problem while retrieving clientId. Client ID might be empty or null.	Provide Client Id.
SPE-5126	There was a problem while retrieving clientSecret. Client Secret might be empty or null.	Provide Client Secret.
SPE-5127	There was a problem while retrieving tenantId. Tenant ID might be empty or null.	Provide Tenant Id.
SPE-5128	There was a problem while retrieving siteUrls. Site URLs might be empty or null.	Provide at least one Site Url.

Error code	Error message	Suggested resolution
SPE-5129	There was a problem while retrieving password. Password might be empty or null.	Provide password.
SPE-5130	There was a problem while retrieving username.Username might be empty or null.	Provide username.
SPE-5131	There was a problem while retrieving username. Email was invalid.	Provide valid email address.
SPE-5132	There was a problem while retrieving url. This URL was invalid.	Provide a valid URL.
SPE-5133	There was a problem while retrieving s3CertificateName. S3 Certificate Name might be empty or null.	Ensure s3CertificateName is not null or non-empty.
SPE-5134	There was a problem while retrieving s3BucketName. S3 Bucket Name might be empty or null	Ensure s3BucketName is not null or non-empty.
SPE-5135	The provided version was not a valid Sharepoint Connector version. Version should be one of [Online, Server].	Version should be one of [Online, Server].

Error code	Error message	Suggested resolution
SPE-5136	The provided authType was not a valid Sharepoint Connector authentication method.	Provide valid authType. The value of authType should be one of [Basic, OAuth2Certificate, OAuth2].
SPE-5138	There was a problem while retrieving onPremVersion. On prem Version might be empty or null	Ensure onPremVersion is not be null or non-empty.
SPE-5139	The provided onPremVersion was not valid Sharepoint on-prem version. On prem version should be one of [2013, 2016, 2019, SubscriptionEdition].	Provide a valid onPremVersion. On prem version should be one of [2013, 2016, 2019, SubscriptionEdition].
SPE-5140	There was a problem while retrieving ldapUrl. LDAP Url might be empty or null.	Ensure ldapUrl is not null or empty.
SPE-5141	There was a problem while retrieving baseDn. Base DN might be empty or null.	Ensure baseDn is not be null or empty.
SPE-5142	There was a problem while retrieving privateKey. Private Key might be empty or null.	Please ensure privateKey is not be null or empty.

Error code	Error message	Suggested resolution
SPE-5144	There was a problem while retrieving aclConfig uration. ACL Configura tion might be empty, null or invalid	Provide valid aclConfiguration. aclConfiguration should be one of [ACLWithLDAPEmailFmt, ACLWithMa nualEmailFmt, ACLWithUsernameFmt].
SPE-5145	There was a problem while retrieving emailDomain. Email Domain might be empty or null.	Ensure emailDomain is not null or empty.
SPE-5146	There was a problem while retrieving ldapUsername. LDAP Username might be empty or null.	Ensure ldapUser is not null or empty.
SPE-5147	There was a problem while retrieving ldapPassword. LDAP Password might be empty or null.	Ensure ldapPassword is not null or empty.
SPE-5149	The provided siteUrls contain duplicate sites. Remove duplicates.	Ensure SiteUrls must not be the same.
SPE-5150	Invalid Client Id pattern.	Provide the correct client ID.
SPE-5151	Error parsing the field value. Size is over maximum allowed limit.	Ensure the size limit.

Error code	Error message	Suggested resolution
SPE-5152	There was a problem while retrieving AD Client ID. AD Client ID should not be empty.	Ensure AD Client Id must be non-empty .
SPE-5153	Invalid AD Client Id pattern.	Provide valid AD Client Id pattern.
SPE-5154	There was a problem while retrieving AD Client Secret. AD Client Secret should not be empty.	Ensure AD Client Secret is non-empty.
SPE-5155	There can't be more than one site for SharePoin t on-prem app-only authentication.	Ensure that their must be only single site present for SharePoint on-prem app-only authentication.
SPE-5200	There was a problem while connecting to the URL.	Ensure the siteUrl exists.

Connecting SharePoint Server (Subscription Edition) to Amazon Q Business

Microsoft SharePoint is a collaborative website building service that lets you customize web content and create web pages, web sites, document libraries, and lists. You can connect a SharePoint Server (Subscription Edition) instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Amazon Q supports Microsoft SharePoint Server (2016, 2019, and Subscription Edition).

Topics

- Known limitations for the Amazon Q Business SharePoint Server (Subscription Edition) connector
- SharePoint Server (Subscription Edition) connector overview
- Prerequisites for connecting Amazon Q Business to SharePoint Server (Subscription Edition)

- Connecting Amazon Q Business to SharePoint Server (Subscription Edition) using the console
- Connecting Amazon Q Business to SharePoint Server (Subscription Edition) using APIs
- Connecting Amazon Q Business to SharePoint Server (Subscription Edition) using AWS CloudFormation
- How Amazon Q Business connector crawls SharePoint Server (Subscription Edition) ACLs
- Amazon Q Business SharePoint Server (Subscription Edition) data source connector field mappings
- IAM role for Amazon Q Business SharePoint Server (Subscription Edition) connector
- Understand error codes in the SharePoint Server (Subscription Edition) connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Amazon Q Business SharePoint Server (Subscription Edition) connector

The SharePoint Server (Subscription Edition) connector has the following known limitations:

- The Amazon Q SharePoint connector supports custom field mappings only for the **Files** entity.
- For all SharePoint Server versions, the ACL token must be in lower case. For **Email with Domain from IDP** and **Email ID with Custom Domain** ACL, for example: *`user@sharepoint2019.com`*. For **Domain\User with Domain** ACL, for example: *`sharepoint2013\user`*.
- If an entity name has a `%` character in its name, the connector will skip these files due to API limitations.
- OneNote can only be crawled by the connector using a Tenant ID, and with OAuth 2.0, OAuth 2.0 refresh token, or SharePoint App Only authentication activated for SharePoint Online.

- The connector crawls the first section of a OneNote document using its default name only, even if the document is renamed.
- The connector crawls links in Subscription Edition, only if **Pages** and **Files** are selected as entities to be crawled in addition to **Links**.
- The connector crawls only list attachments and comments when **List Data** is also selected as an entity to be crawled.
- The connector crawls event attachments only when **Events** is also selected as an entity to be crawled.
- To crawl nested groups using **Identity crawler**, you have to activate Local as well as AD Group Crawling.
- To use **Identity Crawler** with SharePoint Server (Subscription Edition) to crawl nested groups, you have to enable both Local and AD Group Crawling.
- Query responses based on AD Group ACLs are not supported for SharePoint Server (Subscription Edition). You need to add users and groups directly to your document permissions list.
- When Access Control Lists (ACLs) are enabled, the "Sync only new or modified content" option is not available due to SharePoint Server (Subscription Edition) API limitations. We recommend using "Full sync" or "New, modified, or deleted content sync" modes instead, or disable ACLs if you need to use this sync mode.

SharePoint Server (Subscription Edition) connector overview

The following table gives an overview of the Amazon Q Business SharePoint Server (Subscription Edition) connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	NTLM, Kerberos, SharePoint App-Only (Client Credentials Flow)
	Authentication credentials	**NTLM** • SharePoint admin username • SharePoint admin password

Category	Feature	Support
		If you're using **Email ID with Domain from IDP** to crawl ACLs, then you also need to add a: • LDAP Server Endpoint • LDAP Search Base • LDAP username • LDAP password **Kerberos** • SharePoint admin username • SharePoint admin password If you're using **Email ID with Domain from IDP** to crawl ACLs, then you also need to add a: • LDAP Server Endpoint • LDAP Search Base • LDAP username • LDAP password **SharePoint App-Only (Client Credentials Flow)** • Tenant ID • SharePoint App-Only client ID • SharePoint App-Only client secret If you're using **Email ID with Domain from IDP** to crawl ACLs, then you also need to add a:

Category	Feature	Support
		• LDAP Server Endpoint • LDAP Search Base • LDAP username • LDAP password
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Integration with Identity Provider (IdP)	Yes. LDAP.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	Yes. Supports custom metadata for **File** entity only.
	Entities	Yes. The following entities are supported: • Files • Attachments • Link • Pages • Events • Comments See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.

Category	Feature	Support
	Filters	Yes. The following filters are supported: • Include/exclude by **Links** • Include/exclude by **Pages** • Include/exclude by **Events** • Include/exclude by file name • Include/exclude by file path • Include/exclude by file type • Include/exclude by **OneNote Section** name • Include/exclude by **OneNote Page** name
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to SharePoint Server (Subscription Edition)

The following page outlines the prerequisites you need to complete before connecting SharePoint Server (Subscription Edition) to Amazon Q, based on the authentication mode of your choice.

Topics

- Prerequisites for using NTLM authentication
- Prerequisites for using Kerberos authentication
- Prerequisites for using SharePoint App-Only authentication

Prerequisites for using NTLM authentication

If you're using NTLM authentication, make sure you've completed the following steps in SharePoint Server (Subscription Edition):

- Copied your SharePoint instance URLs. The format for the host URL you enter is *`https://yourdomain.sharepoint.com/sites/mysite`*. Your URL must start with `https` and contain `sharepoint.com`.
- Copied the domain name of your SharePoint instance URL.

- Generated an SSL certificate and uploaded it to an Amazon S3 bucket.
- Noted the username and password that you use to connect to SharePoint.

(Optional) If you're using Email ID with Domain from IDP to control access to your documents, make sure you've completed the following steps:

- Copied your LDAP Server Endpoint (endpoint of LDAP server including protocol and port number). For example: *`ldap://example.com:389`*.
- Copied your LDAP Search Base (search base of the LDAP user). For example: *`CN=Users,DC=sharepoint,DC=com`*.
- Copied your LDAP username and LDAP password.

(Optional) If using Email ID with Custom Domain for access control, complete the following step:

- Noted your custom email domain value—for example: *`"amazon.com"`*.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your SharePoint Server (Subscription Edition) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Prerequisites for using Kerberos authentication

If you're using Kerberos authentication, make sure you've completed the following steps in SharePoint Server (Subscription Edition):

- Copied your SharePoint instance URLs. The format for the host URL you enter is *`https://yourdomain.sharepoint.com/sites/mysite`*. Your URL must start with `https` and contain `sharepoint.com`.
- Copied the domain name of your SharePoint instance URL.
- Generated an SSL certificate and uploaded it to an Amazon S3 bucket.
- Noted the username and password that you use to connect to SharePoint.

(Optional) If you're using Email ID with Domain from IDP to control access to your documents, make sure you've completed the following steps:

- Copied your LDAP Server Endpoint (endpoint of LDAP server including protocol and port number). For example: *`ldap://example.com:389`*.
- Copied your LDAP Search Base (search base of the LDAP user). For example: *`CN=Users,DC=sharepoint,DC=com`*.
- Copied your LDAP username and LDAP password.

(Optional) If using Email ID with Custom Domain for access control, complete the following step:

- Noted your custom email domain value—for example: *`"amazon.com"`*.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your SharePoint Server (Subscription Edition) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Prerequisites for using SharePoint App-Only authentication

If you're using SharePoint App-Only authentication, make sure you've completed the following steps in SharePoint Server (Subscription Edition):

- Copied the SharePoint client ID generated when you registered App Only at Site Level. ClientID format is ClientID@TenantId. For example, *ffa956f3-8f89-44e7-b0e4-49670756342c@888d0b57-69f1-4fb8-957f-e1f0bedf82fe*.
- Copied the SharePoint client secret generated when you registered App Only at Site Level.

> **Important**
>
> **Note:** Because client IDs and client secrets are generated for single sites only when you register SharePoint Server for App Only authentication, only one site URL is supported for SharePoint App Only authentication.

- Noted the Tenant ID of your SharePoint Server (Subscription Edition) account.
- Noted your **LDAP Server Endpoint**, **LDAP Search Base**, **LDAP username**, and **LDAP password**.

> **Note**
>
> SharePoint App-Only Authentication is *not* supported for SharePoint 2013 version.

(Optional) If you're using Email ID with Domain from IDP to control access to your documents, make sure you've completed the following steps:

- Copied your LDAP Server Endpoint (endpoint of LDAP server including protocol and port number). For example: *ldap://example.com:389*.
- Copied your LDAP Search Base (search base of the LDAP user). For example: *CN=Users,DC=sharepoint,DC=com*.
- Copied your LDAP username and LDAP password.

(Optional) If using Email ID with Custom Domain for access control, complete the following step:

- Noted your custom email domain value—for example: *"amazon.com"*.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your SharePoint Server (Subscription Edition) authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to SharePoint Server (Subscription Edition) using the console

The following procedure outlines how to connect Amazon Q Business to SharePoint Server (Subscription Edition) using the AWS Management Console.

Connecting Amazon Q to SharePoint Server (Subscription Edition)

1. Sign in to the AWS Management Console and open the Amazon Q Business console.

2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **SharePoint** data source to your Amazon Q application.
5. Then, on the **SharePoint Server (Subscription Edition)** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. In **Source**, enter the following information:

   a. In **Source**, for **Hosting Method** – Choose **SharePoint Server**.

   b. **Choose SharePoint Version** – Choose **SharePoint (Subscription Edition)**.

   c. **Site URLs specific to your SharePoint repository** – Enter the SharePoint host URLs. The format for the host URLs you enter is *`https://yourcompany/sites/mysite`*. The URL must start with `https` protocol. Separate URLs with a new line. You can add up to 100 URLs.

   d. **Domain** – Enter the SharePoint domain.

   e. **SSL certificate location** – Enter the Amazon S3 path to your SSL certificate file.

8. For **Web proxy – *optional*** – Enter the host name (without the `http://` or `https://` protocol), and the port number used by the host URL transport protocol. The numeric value of the port number must be between 0 and 65535.
9. For **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. You can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled

for more details. See Authorization for more details. For SharePoint Server, you can choose from the following ACL options:

a. **Email ID with Domain from IDP** – Access control is based on email IDs that are extracted from email domains fetched from the underlying identity provider (IdP). You provide the IdP connection details in your Secrets Manager secret during **Authentication**.

b. **Email ID with Custom Domain** – Access control is based on email IDs. Provide the email domain value. For example, *"amazon.com"*. The email domain is used to construct the email ID for access control. You must enter your email domain using **Add Email Domain**.

See Authorization for more details.

10. For **Authentication**, choose between **SharePoint App-Only authentication**, **NTLM authentication**, and **Kerberos authentication**, based on your use case.

    a. Enter the following information for both **NTLM authentication** and **Kerberos authentication**:

    For **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your SharePoint authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens. Enter the following information in the window:

    - **Secret name** – A name for your secret.
    - **Username** – Username for your SharePoint account.
    - **Password** – Password for your SharePoint account.

    If using **Email ID with Domain from IDP**, also enter your:

    - **LDAP Server Endpoint** – Endpoint of LDAP server, including protocol and port number. For example: *ldap://example.com:389*.
    - **LDAP Search Base** – Search base of LDAP user. For example: *CN=Users,DC=sharepoint,DC=com*.
    - **LDAP username** – Your LDAP username.
    - **LDAP Password** – Your LDAP password.

    b. Enter the following information for **SharePoint App-Only authentication**:

For **AWS Secrets Manager secret** – Choose an existing secret or create a Secrets Manager secret to store your SharePoint authentication credentials. If you choose to create a secret, an AWS Secrets Manager secret window opens. Enter the following information in the window:

- **Secret name** – A name for your secret.
- **Client ID** – The SharePoint client ID that you generated when you registered App Only at Site Level. The ClientID format is ClientID@TenantId. For example, *ffa956f3-8f89-44e7-b0e4-49670756342c@888d0b57-69f1-4fb8-957f-e1f0bedf82fe*.
- **SharePoint client secret** – The SharePoint client secret generated when your register for App Only at Site Level.

  Note: Because client IDs and client secrets are generated for single sites only when you register SharePoint Server for App Only authentication, only one site URL is supported for SharePoint App Only authentication.

If using **Email ID with Domain from IDP**, also enter your:

- **LDAP Server Endpoint** – Endpoint of LDAP server, including protocol and port number. For example: *ldap://example.com:389*.
- **LDAP Search Base** – Search base of LDAP user. For example: *CN=Users,DC=sharepoint,DC=com*.
- **LDAP username** – Your LDAP user name.
- **LDAP Password** – Your LDAP password.

11. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

12. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.

13. In **Sync scope**, choose from the following options :

    a. **Select entities** – Choose the entities that you want to crawl. You can select to crawl **All** entities or any combination of **Files**, **Attachments**, **Links**, **Pages**, **Events** and **List Data**.

    b. In **Additional configuration – *optional***, for **Entity regex patterns** – Add regular expression patterns for **Links**, **Pages**, and **Events** to include specific entities instead of syncing all your documents.

    c. **Regex patterns** – Add regular expression patterns to include or exclude files by **File path**, **File name**, **File type**, **OneNote section name**, and **OneNote page name** instead of syncing all your documents. You can add up to 100 patterns.

    > **Note**
    >
    > Any valid regex pattern is supported. For example, if you use the regex `^QBusiness*`, any content starting with the word `QBusiness` followed by any number of characters will be filtered (`QBusiness_doc1` or `QBusiness`, but not `doc1_QBusiness`).

    d. **Advanced settings**

    Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

14. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

- **Full sync** – Sync all content regardless of the previous sync status.
- **New or modified content sync** – Sync only new and modified documents.
- **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

For more details, see Sync mode.

15. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
16. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
17. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

18. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Right after setup, Amazon Q Business automatically tests your connection. This test will ensure that your data source connects properly before you run a sync job.

The test process can take 3-5 minutes. The console will show you if your test is successful. If the test fails, it will display a message.

> **Important**
>
> Amazon Q Business can only surface one error at a time. After you correct an error, the test automatically runs again. If there is another error, you will see a message.

Connecting Amazon Q Business to SharePoint Server (Subscription Edition) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- SharePoint Server (Subscription Edition) configuration properties
- SharePoint Server (Subscription Edition) JSON schema

- SharePoint Server (Subscription Edition) JSON schema example

SharePoint Server (Subscription Edition) configuration properties

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-properties. • `siteUrls` • `domain` • `repositoryAdditionalProperties` • `tenantId`	Yes
`tenantId`	The tenant id of your SharePoint account.	`string` OAuth2 series required	Yes
`domain`	The domain of your SharePoint account.	`string`	Yes
`siteUrls`	The host URLs of your SharePoint account.	`array (string)`	Yes

Configuration	Description	Type	Required
		Specify the URL in the pattern `https://*`	
`repositoryAdditionalProperties`	Additional properties to connect with your repository endpoint.	`object` This property has the following sub-properties. • `version` • `authType` • `onPremVersion`	Yes
`authType`	The type of authentication you are using: `NTLM`, `Kerberos`, or `OAuth2App` .	`string`	Yes
`version`	The SharePoint version you are using: `Sever`.	`string (Server)`	Yes
`onPremVersion`	The SharePoint version that you are using.	`string` Valid values are (empty), `2013`, `2016`, `2019`, and `SubscriptionEdition` .	Yes

Configuration	Description	Type	Required
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties. • `event` • `page` • `file` • `link` • `attachment` • `comment`	Yes
• `event` • `page` • `file` • `link` • `attachment` • `comment`	A list of objects that map the attributes or field names of your SharePoint Server (Subscription Edition) pages and assets to Amazon Q index field names.	`object` These properties have the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName` • `dateFieldFormat`	No

Configuration	Description	Type	Required
`indexFieldName`	The field name of your SharePoint Server (Subscription Edition) events, pages, files, links, attachments, or comments.	`string`	Yes
`indexFieldType`	The field type of your SharePoint Server (Subscription Edition) events, pages, files, links, attachments, or comments.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes
`dataSourceFieldName`	The data source field name of your SharePoint Server (Subscription Edition) events, pages, files, links, attachments, or comments.	`string`	Yes
`dateFieldFormat`	The date format of your SharePoint Server (Subscription Edition) events, pages, files, links, attachments, or comments.	`string` Specify the date format in the form `yyyy-MM-dd"T"HH:mm:ss"Z"`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties: • crawlAcl • crawlFiles • crawlPages • crawlEvents • crawlComments • crawlLinks • crawlAttachments • crawlListData • isCrawlLocalGroupMapping • isCrawlAdGroupMapping • aclConfiguration • emailDomain • maxFileSizeInMegaBytes • eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx	Yes

Configuration	Description	Type	Required
		• inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotePageNamePatterns	

Configuration	Description	Type	Required
		• `proxyHost` • `proxyPort`	

Configuration	Description	Type	Required
• eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePa	A list of regular expression patterns to include/exclude specific files in your SharePoint data source. Files that match the patterns are included in the index. File that don&t match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn&t included in the index.	array (string)	No

Configuration	Description	Type	Required
geNamePat terns • exclusion OneNotePa geNamePat terns • emailDomain			
aclConfig uration	Specifes how your ACL is configured.	string> Valid values are ACLWithLD APEmailFm t , ACLWithMa nualEmailFmt , or ACLWithUs ernameFmt .	No
proxyHost	The host where the web proxy is required. The host name should be without protocol (http:// or https://).	string	Yes
proxyPort	Port used by the host URL transport protocol. The port number should be a numeric value between 0 and 65535.	string	Yes

Configuration	Description	Type	Required
• crawlAcl • crawlFiles • crawlPages • crawlEvents • crawlComments • crawlLinks • crawlAttachments • crawlListData • isCrawlLocalGroupMapping • isCrawlAdGroupMapping	Input TRUE to index.	boolean	No
maxFileSizeInMegaBytes	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	string	No

Configuration	Description	Type	Required
`sslCertificatePath`	Configuration information to access the SSL certificate stored in your Amazon S3 bucket.	`object` This property has the following sub-properties. • `bucket` • `key`	No
`bucket`	The name of the Amazon S3 bucket that stores your Microsoft Entra ID (formerly Azure AD) self-signed X.509 certificate.	`string`	Yes
`key`	The name of the SSL certificate stored in your Amazon S3 bucket.	`string`	Yes
`type`	We recommend that you use `SHAREPOINTV2` as your data source type.	`string` Valid values are `SHAREPOINTV2` and `SHAREPOINT`.	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. See Identity crawler for more information.	`boolean`	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index	Yes

Configuration	Description	Type	Required
secretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your SharePoint. If you use OAuth2App authentication, provide the client ID, client secret, LDAP URL, LDAP base DN, LDAP user name, and LDAP password. If you use NTLM or Kerberos authentication, provide the user name, password, LDAP URL, Base DN, LDAP user, and LDAP password.	string The minimum length is 20 and the maximum length is 2,048 characters. If you use Sharepoint App-Only authentication (authType should be 0Auth2App authentication) the secret must contain a JSON structure with the following keys: { "clientId": "client ID", "clientSecret": " client secret", "ldapUrl": "LDAP URL", "ldbaseDn": "LDAP base DN", "ldapUser": " LDAP user name", "ldapPassword": " LDAP password" } If you use NTLM authentication or Kerberos authentic	Yes

Configuration	Description	Type	Required
		ation, the secret must contain a JSON structure with the following keys: `{ "userName": "SharePoint account user name", "password": " SharePoint account password", "ldapUrl": "LDAP URL", "baseDn": "LDAP base DN", "ldapUser": " LDAP user name", "ldapPassword": " LDAP password" }`	
`version`	The version of this template that&s currently supported.	`string`	No

SharePoint Server (Subscription Edition) JSON schema

The following is the SharePoint Server (Subscription Edition) JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
```

```
      "enum": ["SHAREPOINTV2", "SHAREPOINT"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "sslCertificatePath": {
      "type": "object",
      "properties": {
        "bucket": {
          "type": "string",
          "pattern": "^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$",
          "minLength": 3,
          "maxLength": 63
        },
        "key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 10240
        }
      },
      "required": ["bucket", "key"]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
```

```
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            },
            "domain": {
              "type": "string"
            },
            "siteUrls": {
              "type": "array",
              "items": {
                "type": "string",
                "pattern": "https://.*"
              }
            },
            "repositoryAdditionalProperties": {
              "type": "object",
              "properties": {
                "authType": {
                  "type": "string",
                  "enum": ["OAuth2App", "NTLM", "Kerberos"]
                },
                "version": {
                  "type": "string",
                  "enum": ["Server"]
                },
                "onPremVersion": {
                  "type": "string",
                  "enum": ["", "2013", "2016", "2019", "SubscriptionEdition"]
                },
                "enableDeletionProtection": {
                  "anyOf": [
                    {
                      "type": "boolean"
                    },
                    {
                      "type": "string",
                      "enum": ["true", "false"]
                    }
                  ],
                  "default": false
```

```
              },
              "deletionProtectionThreshold": {
                "type": "string",
                "default": "15"
              }
            },
            "required": ["authType", "version"]
          }
        },
        "required": ["siteUrls", "domain", "repositoryAdditionalProperties"]
      }
    },
    "required": ["repositoryEndpointMetadata"]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "event": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
```

```
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "page": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "file": {
```

```
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "link": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "attachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
```

```
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "comment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
```

```
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "eventTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "pageTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "linkTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionFilePath": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionFilePath": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionFileTypePatterns": {
        "type": "array",
```

```
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionOneNoteSectionNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionOneNoteSectionNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionOneNotePageNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionOneNotePageNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
```

```
          }
        },
        "crawlFiles": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlPages": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlEvents": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlComments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
```

```
          ]
        },
        "crawlLinks": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAttachments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlListData": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
```

```
          ]
        },
        "aclConfiguration": {
          "type": "string",
          "enum": [
            "ACLWithLDAPEmailFmt",
            "ACLWithManualEmailFmt",
            "ACLWithUsernameFmt"
          ]
        },
        "emailDomain": {
          "type": "string"
        },
        "isCrawlLocalGroupMapping": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlAdGroupMapping": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "proxyHost": {
          "type": "string"
        },
        "proxyPort": {
          "type": "string"
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        }
```

```
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "type",
    "secretArn",
    "syncMode",
    "enableIdentityCrawler",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

SharePoint Server (Subscription Edition) JSON schema example

The following is the SharePoint Server (Subscription Edition) JSON schema example:

```
{

  "type": "SHAREPOINTV2",

  "syncMode": "FULL_CRAWL",

  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-sharepoint-
secret",

  "enableIdentityCrawler": "true",

  "sslCertificatePath": {

    "bucket": "my-sharepoint-bucket",

    "key": "ssl/cert.pem"
```

```
  },
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "tenantId": "1234567a-890b-1234-567c-123456789012",
      "domain": "mycompany.sharepoint.com",
      "siteUrls": [
        "https://mycompany.sharepoint.com/sites/TeamSite"
      ],
      "repositoryAdditionalProperties": {
        "authType": "OAuth2",
        "version": "Server",
        "onPremVersion": "2019",
        "enableDeletionProtection": "false",
        "deletionProtectionThreshold": "15"
      }
    }
  },
  "repositoryConfigurations": {
    "event": {
      "fieldMappings": [
        {
          "indexFieldName": "event_id",
          "indexFieldType": "STRING",
```

```
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    ]
  },
  "page": {
    "fieldMappings": [
      {
        "indexFieldName": "page_id",
        "indexFieldType": "STRING",
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    ]
  },
  "file": {
    "fieldMappings": [
      {
        "indexFieldName": "file_id",
        "indexFieldType": "STRING",
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
```

```
        }
      ]
    },
    "link": {
      "fieldMappings": [
        {
          "indexFieldName": "link_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "attachment": {
      "fieldMappings": [
        {
          "indexFieldName": "attachment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
```

```
    },

    "comment": {

      "fieldMappings": [

        {

          "indexFieldName": "comment_id",

          "indexFieldType": "STRING",

          "dataSourceFieldName": "id",

          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"

        }

      ]

    }

  },

  "additionalProperties": {

    "eventTitleFilterRegEx": [
      "^.*$"
    ],

    "pageTitleFilterRegEx": [
      "^.*$"
    ],

    "linkTitleFilterRegEx": [
      "^.*$"
    ],

    "inclusionFilePath": [
      "documents/"
    ],

    "exclusionFilePath": [
      "drafts/"
```

```
    ],

    "inclusionFileTypePatterns": [
      "*.pdf",
       "*.docx"
    ],

    "exclusionFileTypePatterns": [
      "*.tmp"
    ],

    "inclusionFileNamePatterns": [
      "*report*"
    ],

    "exclusionFileNamePatterns": [
      "*draft*"
    ],

    "inclusionOneNoteSectionNamePatterns": [
      "*"
    ],

    "exclusionOneNoteSectionNamePatterns": [
      "archived"
    ],

    "inclusionOneNotePageNamePatterns": [
      "*"
    ],

    "exclusionOneNotePageNamePatterns": [
      "test"
    ],

    "crawlFiles": "true",

    "crawlPages": "true",

    "crawlEvents": "true",

    "crawlComments": "true",

    "crawlLinks": "true",
```

```
    "crawlAttachments": "true",
    "crawlListData": "false",
    "crawlAcl": "true",
    "aclConfiguration": "ACLWithUsernameFmt",
    "emailDomain": "mycompany.com",
    "isCrawlLocalGroupMapping": "false",
    "isCrawlAdGroupMapping": "true",
    "proxyHost": "proxy.mycompany.com",
    "proxyPort": "8080",
    "maxFileSizeInMegaBytes": "50"
  },
  "version": "1.0.0"
}
```

Connecting Amazon Q Business to SharePoint Server (Subscription Edition) using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- SharePoint Server (Subscription Edition) configuration properties

- SharePoint Server (Subscription Edition) JSON schema for using the configuration property with AWS CloudFormation
- SharePoint Server (Subscription Edition) YAML schema for using the configuration property with AWS CloudFormation

SharePoint Server (Subscription Edition) configuration properties

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-properties. • `siteUrls` • `domain` • `repositoryAdditionalProperties` • `tenantId`	Yes
`tenantId`	The tenant id of your SharePoint account.	`string` OAuth2 series required	Yes
`domain`	The domain of your SharePoint account.	`string`	Yes

Configuration	Description	Type	Required
`siteUrls`	The host URLs of your SharePoint account.	`array (string)` Specify the URL in the pattern `https://*`	Yes
`repositoryAdditionalProperties`	Additional properties to connect with your repository endpoint.	`object` This property has the following sub-properties. • `version` • `authType` • `onPremVersion`	Yes
`authType`	The type of authentication you are using: `NTLM`, `Kerberos`, or `OAuth2App` .	`string`	Yes
`version`	The SharePoint version you are using: `Sever`.	`string (Server)`	Yes
`onPremVersion`	The SharePoint version that you are using.	`string` Valid values are (empty), `2013`, `2016`, `2019`, and `SubscriptionEdition` .	Yes

Configuration	Description	Type	Required
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties. • `event` • `page` • `file` • `link` • `attachment` • `comment`	Yes
• `event` • `page` • `file` • `link` • `attachment` • `comment`	A list of objects that map the attributes or field names of your SharePoint Server (Subscription Edition) pages and assets to Amazon Q index field names.	`object` These properties have the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName` • `dateFieldFormat`	No

Configuration	Description	Type	Required
`indexFieldName`	The field name of your SharePoint Server (Subscription Edition) events, pages, files, links, attachments, or comments.	`string`	Yes
`indexFieldType`	The field type of your SharePoint Server (Subscription Edition) events, pages, files, links, attachments, or comments.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes
`dataSourceFieldName`	The data source field name of your SharePoint Server (Subscription Edition) events, pages, files, links, attachments, or comments.	`string`	Yes
`dateFieldFormat`	The date format of your SharePoint Server (Subscription Edition) events, pages, files, links, attachments, or comments.	`string` Specify the date format in the form `yyyy-MM-dd"T"HH:mm:ss"Z"`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties: • crawlAcl • crawlFiles • crawlPages • crawlEvents • crawlComments • crawlLinks • crawlAttachments • crawlListData • isCrawlLocalGroupMapping • isCrawlAdGroupMapping • aclConfiguration • emailDomain • maxFileSizeInMegaBytes • eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx	Yes

Configuration	Description	Type	Required
		• inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotePageNamePatterns	

Configuration	Description	Type	Required
		• proxyHost • proxyPort	

Configuration	Description	Type	Required
• eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath • inclusionFileTypePatterns • exclusionFileTypePatterns • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePa	A list of regular expression patterns to include/exclude specific files in your SharePoint data source. Files that match the patterns are included in the index. File that don&t match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn&t included in the index.	array (string)	No

Configuration	Description	Type	Required
geNamePat terns • exclusion OneNotePa geNamePat terns • emailDomain			
aclConfig uration	Specifes how your ACL is configured.	string> Valid values are ACLWithLD APEmailFm t , ACLWithMa nualEmailFmt , or ACLWithUs ernameFmt .	No
proxyHost	The host where the web proxy is required. The host name should be without protocol (http:// or https://).	string	Yes
proxyPort	Port used by the host URL transport protocol. The port number should be a numeric value between 0 and 65535.	string	Yes

Configuration	Description	Type	Required
• crawlAcl • crawlFiles • crawlPages • crawlEvents • crawlComments • crawlLinks • crawlAttachments • crawlListData • isCrawlLocalGroupMapping • isCrawlAdGroupMapping	Input TRUE to index.	boolean	No
maxFileSizeInMegaBytes	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	string	No

Configuration	Description	Type	Required
`sslCertificatePath`	Configuration information to access the SSL certificate stored in your Amazon S3 bucket.	`object` This property has the following sub-properties. • `bucket` • `key`	No
`bucket`	The name of the Amazon S3 bucket that stores your Microsoft Entra ID (formerly Azure AD) self-signed X.509 certificate.	`string`	Yes
`key`	The name of the SSL certificate stored in your Amazon S3 bucket.	`string`	Yes
`type`	We recommend that you use `SHAREPOINTV2` as your data source type.	`string` Valid values are `SHAREPOINTV2` and `SHAREPOINT`.	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. See Identity crawler for more information.	`boolean`	Yes

Configuration	Description	Type	Required
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index	Yes

Configuration	Description	Type	Required
secretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your SharePoint. If you use OAuth2App authentication, provide the client ID, client secret, LDAP URL, LDAP base DN, LDAP user name, and LDAP password. If you use NTLM or Kerberos authentication, provide the user name, password, LDAP URL, Base DN, LDAP user, and LDAP password.	string The minimum length is 20 and the maximum length is 2,048 characters. If you use Sharepoint App-Only authentication (authType should be 0Auth2App authentication) the secret must contain a JSON structure with the following keys: { "clientId": "*client ID*", "clientSecret": " *client secret*", "ldapUrl": "*LDAP URL*", "ldbaseDn": "*LDAP base DN*", "ldapUser": " *LDAP user name*", "ldapPassword": " *LDAP password*" } If you use NTLM authentication or Kerberos authentic	Yes

Configuration	Description	Type	Required
		ation, the secret must contain a JSON structure with the following keys: `{ "userName": "SharePoint account user name", "password": " SharePoint account password", "ldapUrl": "LDAP URL", "baseDn": "LDAP base DN", "ldapUser": " LDAP user name", "ldapPassword": " LDAP password" }`	
`version`	The version of this template that&s currently supported.	`string`	No

SharePoint Server (Subscription Edition) JSON schema for using the configuration property with AWS CloudFormation

The following is the SharePoint Server (Subscription Edition) JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- SharePoint Server (Subscription Edition) JSON schema for using the configuration property with AWS CloudFormation
- SharePoint Server (Subscription Edition) JSON schema example for using the configuration property with AWS CloudFormation

SharePoint Server (Subscription Edition) JSON schema for using the configuration property with AWS CloudFormation

The following is the SharePoint Server (Subscription Edition) JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["SHAREPOINTV2", "SHAREPOINT"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "sslCertificatePath": {
      "type": "object",
      "properties": {
        "bucket": {
```

```
          "type": "string",
          "pattern": "^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$",
          "minLength": 3,
          "maxLength": 63
        },
        "key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 10240
        }
      },
      "required": ["bucket", "key"]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            },
            "domain": {
              "type": "string"
            },
            "siteUrls": {
              "type": "array",
              "items": {
                "type": "string",
                "pattern": "https://.*"
              }
            },
            "repositoryAdditionalProperties": {
              "type": "object",
              "properties": {
                "authType": {
                  "type": "string",
                  "enum": ["OAuth2App", "NTLM", "Kerberos"]
                },
                "version": {
```

```
                "type": "string",
                "enum": ["Server"]
              },
              "onPremVersion": {
                "type": "string",
                "enum": ["", "2013", "2016", "2019", "SubscriptionEdition"]
              },
              "enableDeletionProtection": {
                "anyOf": [
                  {
                    "type": "boolean"
                  },
                  {
                    "type": "string",
                    "enum": ["true", "false"]
                  }
                ],
                "default": false
              },
              "deletionProtectionThreshold": {
                "type": "string",
                "default": "15"
              }
            },
            "required": ["authType", "version"]
          }
        },
        "required": ["siteUrls", "domain", "repositoryAdditionalProperties"]
      }
    },
    "required": ["repositoryEndpointMetadata"]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "event": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
```

```
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "page": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
```

```
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "file": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
```

```
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "link": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "attachment": {
```

```
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "comment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "eventTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "pageTitleFilterRegEx": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "linkTitleFilterRegEx": {
        "type": "array",
```

```
          "items": {
            "type": "string"
          }
        },
        "inclusionFilePath": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFilePath": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionOneNoteSectionNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
```

```
        }
      },
      "exclusionOneNoteSectionNamePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionOneNotePageNamePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionOneNotePageNamePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "crawlFiles": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlPages": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "crawlEvents": {
        "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlComments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlLinks": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAttachments": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlListData": {
          "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "crawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "aclConfiguration": {
          "type": "string",
          "enum": [
            "ACLWithLDAPEmailFmt",
            "ACLWithManualEmailFmt",
            "ACLWithUsernameFmt"
          ]
        },
        "emailDomain": {
          "type": "string"
        },
        "isCrawlLocalGroupMapping": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlAdGroupMapping": {
          "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "proxyHost": {
          "type": "string"
        },
        "proxyPort": {
          "type": "string"
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "type",
    "secretArn",
    "syncMode",
    "enableIdentityCrawler",
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties"
  ]
}
```

SharePoint Server (Subscription Edition) JSON schema example for using the configuration property with AWS CloudFormation

The following is the SharePoint Server (Subscription Edition) JSON schema example for the configuration property for CloudFormation

```
{

  "AWSTemplateFormatVersion": "2010-09-09",

  "Description": "CloudFormation SHAREPOINT Data Source Template",

  "Resources": {

    "DataSourceSharePoint": {

      "Type": "AWS::QBusiness::DataSource",

      "Properties": {

        "ApplicationId": "app12345-1234-1234-1234-123456789012",

        "IndexId": "indx1234-1234-1234-1234-123456789012",

        "DisplayName": "MySharePointDataSource",

        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",

        "Configuration": {

          "type": "SHAREPOINTV2",

          "syncMode": "FULL_CRAWL",

          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-
sharepoint-secret",

          "enableIdentityCrawler": "true",

          "sslCertificatePath": {

            "bucket": "my-sharepoint-bucket",
```

```
            "key": "ssl/cert.pem"

          },

          "connectionConfiguration": {

            "repositoryEndpointMetadata": {

              "tenantId": "1234567a-890b-1234-567c-123456789012",

              "domain": "mycompany.sharepoint.com",

              "siteUrls": [
                "https://mycompany.sharepoint.com/sites/TeamSite"
              ],

              "repositoryAdditionalProperties": {

                "authType": "OAuth2",

                "version": "Server",

                "onPremVersion": "2019",

                "enableDeletionProtection": "false",

                "deletionProtectionThreshold": "15"

              }

            }

          },

          "repositoryConfigurations": {

            "event": {

              "fieldMappings": [

                {

                  "indexFieldName": "event_id",
```

```
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "page": {
        "fieldMappings": [
          {
            "indexFieldName": "page_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "file": {
        "fieldMappings": [
          {
            "indexFieldName": "file_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
```

```
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "link": {
        "fieldMappings": [
          {
            "indexFieldName": "link_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        ]
      },
      "attachment": {
        "fieldMappings": [
          {
            "indexFieldName": "attachment_id",
            "indexFieldType": "STRING",
            "dataSourceFieldName": "id",
            "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
```

```
            ]

          },

          "comment": {

            "fieldMappings": [

              {

                "indexFieldName": "comment_id",

                "indexFieldType": "STRING",

                "dataSourceFieldName": "id",

                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"

              }

            ]

          }

        },

        "additionalProperties": {

          "eventTitleFilterRegEx": [
            "^.*$"
          ],

          "pageTitleFilterRegEx": [
            "^.*$"
          ],

          "linkTitleFilterRegEx": [
            "^.*$"
          ],

          "inclusionFilePath": [
            "documents/"
          ],
```

```
            "exclusionFilePath": [
              "drafts/"
            ],

            "inclusionFileTypePatterns": [
              "*.pdf",
               "*.docx"
            ],

            "exclusionFileTypePatterns": [
              "*.tmp"
            ],

            "inclusionFileNamePatterns": [
              "*report*"
            ],

            "exclusionFileNamePatterns": [
              "*draft*"
            ],

            "inclusionOneNoteSectionNamePatterns": [
              "*"
            ],

            "exclusionOneNoteSectionNamePatterns": [
              "archived"
            ],

            "inclusionOneNotePageNamePatterns": [
              "*"
            ],

            "exclusionOneNotePageNamePatterns": [
              "test"
            ],

            "crawlFiles": "true",

            "crawlPages": "true",

            "crawlEvents": "true",

            "crawlComments": "true",
```

```
            "crawlLinks": "true",
            "crawlAttachments": "true",
            "crawlListData": "false",
            "crawlAcl": "true",
            "aclConfiguration": "ACLWithUsernameFmt",
            "emailDomain": "mycompany.com",
            "isCrawlLocalGroupMapping": "false",
            "isCrawlAdGroupMapping": "true",
            "proxyHost": "proxy.mycompany.com",
            "proxyPort": "8080",
            "maxFileSizeInMegaBytes": "50"
          }
        }
      }
    }
  }
}
```

SharePoint Server (Subscription Edition) YAML schema for using the configuration property with AWS CloudFormation

The following is the SharePoint Server (Subscription Edition) YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- SharePoint Server (Subscription Edition) YAML schema for using the configuration property with AWS CloudFormation
- SharePoint Server (Subscription Edition) YAML schema example for using the configuration property with AWS CloudFormation

SharePoint Server (Subscription Edition) YAML schema for using the configuration property with AWS CloudFormation

The following is the SharePoint Server (Subscription Edition) YAML schema for the configuration property for CloudFormation.

```
type: object
properties:
  type:
    type: string
    enum:
      - SHAREPOINTV2
      - SHAREPOINT
  syncMode:
    type: string
    enum:
      - FULL_CRAWL
      - FORCED_FULL_CRAWL
      - CHANGE_LOG
  secretArn:
    type: string
    minLength: 20
    maxLength: 2048
  enableIdentityCrawler:
    anyOf:
      - type: boolean
      - type: string
        enum:
          - true
          - false
  sslCertificatePath:
    type: object
    properties:
      bucket:
        type: string
        pattern: '^[a-z0-9][\\.\\-a-z0-9]{1,61}[a-z0-9]$'
        minLength: 3
```

```
        maxLength: 63
      key:
        type: string
        minLength: 1
        maxLength: 10240
    required:
      - bucket
      - key
  connectionConfiguration:
    type: object
    properties:
      repositoryEndpointMetadata:
        type: object
        properties:
          tenantId:
            type: string
            pattern: "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$"
            minLength: 36
            maxLength: 36
          domain:
            type: string
          siteUrls:
            type: array
            items:
              type: string
              pattern: "https://.*"
          repositoryAdditionalProperties:
            type: object
            properties:
              authType:
                type: string
                enum:
                  - OAuth2App
                  - NTLM
                  - Kerberos
              version:
                type: string
                enum:
                  - Server
              onPremVersion:
                type: string
                enum:
                  - ""
                  - "2013"
```

```
                - "2016"
                - "2019"
                - SubscriptionEdition
            enableDeletionProtection:
              anyOf:
                - type: boolean
                - type: string
                  enum:
                    - true
                    - false
              default: false
            deletionProtectionThreshold:
              type: string
              default: "15"
          required:
            - authType
            - version
      required:
        - siteUrls
        - domain
        - repositoryAdditionalProperties
  required:
    - repositoryEndpointMetadata
repositoryConfigurations:
  type: object
  properties:
    event:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - STRING_LIST
                  - DATE
              dataSourceFieldName:
                type: string
```

```
            dateFieldFormat:
              type: string
              pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
          required:
            - indexFieldName
            - indexFieldType
            - dataSourceFieldName
      required:
        - fieldMappings
    page:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - DATE
                  - LONG
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    file:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
```

```
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - DATE
                  - LONG
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
        required:
          - fieldMappings
      link:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
```

```
        required:
          - fieldMappings
      attachment:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      comment:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
```

```
                  - DATE
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
  required: []
additionalProperties:
  type: object
  properties:
    eventTitleFilterRegEx:
      type: array
      items:
        type: string
    pageTitleFilterRegEx:
      type: array
      items:
        type: string
    linkTitleFilterRegEx:
      type: array
      items:
        type: string
    inclusionFilePath:
      type: array
      items:
        type: string
    exclusionFilePath:
      type: array
      items:
        type: string
    inclusionFileTypePatterns:
      type: array
      items:
        type: string
    exclusionFileTypePatterns:
      type: array
      items:
        type: string
```

```
      inclusionFileNamePatterns:
        type: array
        items:
          type: string
      exclusionFileNamePatterns:
        type: array
        items:
          type: string
      inclusionOneNoteSectionNamePatterns:
        type: array
        items:
          type: string
      exclusionOneNoteSectionNamePatterns:
        type: array
        items:
          type: string
      inclusionOneNotePageNamePatterns:
        type: array
        items:
          type: string
      exclusionOneNotePageNamePatterns:
        type: array
        items:
          type: string
      crawlFiles:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlPages:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlEvents:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
```

```
            - false
      crawlComments:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlLinks:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlAttachments:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlListData:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      crawlAcl:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      aclConfiguration:
        type: string
        enum:
          - ACLWithLDAPEmailFmt
          - ACLWithManualEmailFmt
          - ACLWithUsernameFmt
      emailDomain:
        type: string
```

```
      isCrawlLocalGroupMapping:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      isCrawlAdGroupMapping:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      proxyHost:
        type: string
      proxyPort:
        type: string
      maxFileSizeInMegaBytes:
        type: string
    required: []
  version:
    type: string
    anyOf:
      - pattern: 1.0.0
required:
  - type
  - secretArn
  - syncMode
  - enableIdentityCrawler
  - connectionConfiguration
  - repositoryConfigurations
  - additionalProperties
```

SharePoint Server (Subscription Edition) YAML schema example for using the configuration property with AWS CloudFormation

The following is the SharePoint Server (Subscription Edition) YAML example for the Configuration property for CloudFormation:

```
{
```

```
  "type": "SHAREPOINTV2",

  "syncMode": "FULL_CRAWL",

  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-sharepoint-
secret",

  "enableIdentityCrawler": "true",

  "sslCertificatePath": {

    "bucket": "my-sharepoint-bucket",

    "key": "ssl/cert.pem"

  },

  "connectionConfiguration": {

    "repositoryEndpointMetadata": {

      "tenantId": "1234567a-890b-1234-567c-123456789012",

      "domain": "mycompany.sharepoint.com",

      "siteUrls": [
        "https://mycompany.sharepoint.com/sites/TeamSite"
      ],

      "repositoryAdditionalProperties": {

        "authType": "OAuth2",

        "version": "Server",

        "onPremVersion": "2019",

        "enableDeletionProtection": "false",

        "deletionProtectionThreshold": "15"

      }

    }
```

```
},
"repositoryConfigurations": {
  "event": {
    "fieldMappings": [
      {
        "indexFieldName": "event_id",
        "indexFieldType": "STRING",
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    ]
  },
  "page": {
    "fieldMappings": [
      {
        "indexFieldName": "page_id",
        "indexFieldType": "STRING",
        "dataSourceFieldName": "id",
        "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    ]
  },
```

```
    "file": {
      "fieldMappings": [
        {
          "indexFieldName": "file_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "link": {
      "fieldMappings": [
        {
          "indexFieldName": "link_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "attachment": {
      "fieldMappings": [
```

```
        {
          "indexFieldName": "attachment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "comment": {
      "fieldMappings": [
        {
          "indexFieldName": "comment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    }
  },
  "additionalProperties": {
    "eventTitleFilterRegEx": [
      "^.*$"
    ],
```

```
"pageTitleFilterRegEx": [
  "^.*$"
],

"linkTitleFilterRegEx": [
  "^.*$"
],

"inclusionFilePath": [
  "documents/"
],

"exclusionFilePath": [
  "drafts/"
],

"inclusionFileTypePatterns": [
  "*.pdf",
   "*.docx"
],

"exclusionFileTypePatterns": [
  "*.tmp"
],

"inclusionFileNamePatterns": [
  "*report*"
],

"exclusionFileNamePatterns": [
  "*draft*"
],

"inclusionOneNoteSectionNamePatterns": [
  "*"
],

"exclusionOneNoteSectionNamePatterns": [
  "archived"
],

"inclusionOneNotePageNamePatterns": [
  "*"
```

```
    ],

    "exclusionOneNotePageNamePatterns": [
      "test"
    ],

    "crawlFiles": "true",

    "crawlPages": "true",

    "crawlEvents": "true",

    "crawlComments": "true",

    "crawlLinks": "true",

    "crawlAttachments": "true",

    "crawlListData": "false",

    "crawlAcl": "true",

    "aclConfiguration": "ACLWithUsernameFmt",

    "emailDomain": "mycompany.com",

    "isCrawlLocalGroupMapping": "false",

    "isCrawlAdGroupMapping": "true",

    "proxyHost": "proxy.mycompany.com",

    "proxyPort": "8080",

    "maxFileSizeInMegaBytes": "50"

  },

  "version": "1.0.0"

}
```

How Amazon Q Business connector crawls SharePoint Server (Subscription Edition) ACLs

When you connect an SharePoint Server (Subscription Edition) data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your SharePoint Server (Subscription Edition) instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

To filter using a username, use the **User principal name** from your Azure portal. For example, johnstiles@kendra.onmicrosoft.com.

When you use a SharePoint group for user context filtering, calculate the group ID as follows:

For local groups

1. Get the site name. For example, `https://host.onmicrosoft.com/sites/siteName`.
2. Take the SHA256 hash of the site name. For example, `430a6b90503eef95c89295c8999c7981`.
3. Create the group ID by concatenating the SHA256 hash with a vertical bar (|) and the group name. For example, if the group name is "local group name", the group ID is the following:

   `"430a6b90503eef95c89295c8999c7981 | localGroupName"` (with a space before and after the vertical bar).

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Amazon Q Business SharePoint Server (Subscription Edition) data source connector field mappings

To help you structure data for retrieval and chat filtering, Amazon Q Business crawls data source document attributes or metadata and maps them to fields in your Amazon Q index.

Amazon Q has reserved fields that it uses when querying your application. When possible, Amazon Q automatically maps these built-in fields to attributes in your data source. If a built-in field doesn't have a default mapping, or if you want to map additional index fields, use the custom field

mappings to specify how a data source attribute maps to your Amazon Q application. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

Important

Filtering using document attributes in chat is only supported through the API.

The Amazon Q SharePoint connector supports the following entities and the associated reserved and custom attributes.

Important

If you map any SharePoint Server (Subscription Edition) field to Amazon Q document title and document body fields, Amazon Q will generate responses from data in the document title and body.

Note

You can map any SharePoint field to the document title or document body Amazon Q reserved/default index fields.

Supported entities and field mappings

- Files
- Events
- Pages
- Links
- Attachments
- Comments

Files

SharePoint field name	Index field name	Description	Data type
title	sp_title	Custom	String
sourceUri	_source_uri	Default	String
checkInComment	sp_checkInComment	Custom	String
size	sp_sizeLong	Custom	Long (numeric)
lastModifiedDateTime	_last_updated_at	Default	Date
createdAt	_created_at	Default	Date
author	_authors	Default	String list
majorVersion	sp_majorVersion	Custom	String
uiVersionLabel	sp_uiVersionLabel	Custom	String
uniqueId	sp_uniqueId	Custom	String
irmEnabled	sp_irmEnabled	Custom	String
checkOutType	sp_checkOutType	Custom	String
category	_category	Default	String
modifiedBy	sp_modifiedBy	Custom	String
level	sp_level	Custom	String
uiVersion	sp_uiVersion	Custom	String
contentTag	sp_contentTag	Custom	String
eTag	sp_eTag	Custom	String

SharePoint field name	Index field name	Description	Data type
oneNoteDocument	sp_oneNoteDocument	Custom	String
oneNoteSection	sp_oneNoteSection	Custom	String
oneNotePage	sp_oneNotePage	Custom	String

Events

SharePoint field name	Index field name	Description	Data type
title	sp_title	Custom	String
lastModifiedDateTime	_last_updated_at	Default	Date
sourceUri	_source_uri	Default	String
attachments	sp_hasAttachments	Custom	String
createdDate	_created_at	Default	Date
authorId	sp_authorId	Custom	String
editorId	sp_editorId	Custom	String
location	sp_location	Custom	String
eventDate	sp_eventDate	Custom	Date
eventEndDate	sp_eventEndDate	Custom	Date
ifRecurrence	sp_ifRecurrence	Custom	String
ifAllDayEvent	sp_ifAllDayEvent	Custom	String

SharePoint field name	Index field name	Description	Data type
category	_category	Default	String
eventCategory	sp_eventcategory	Custom	String

Pages

SharePoint field name	Index field name	Description	Data type
createdDateTime	_created_at	Default	Date
lastModifiedDateTime	_last_updated_at	Default	Date
title	sp_title	Custom	String
sourceUri	_source_uri	Default	String
firstPublishedDate	sp_firstPublishedDate	Custom	Date
authorId	sp_authorId	Custom	String
editorId	sp_editorId	Custom	String
category	_category	Default	String

Links

SharePoint field name	Index field name	Description	Data type
createdAt	_created_at	Default	Date
lastModifiedDateTime	_last_updated_at	Default	Date

SharePoint field name	Index field name	Description	Data type
title	sp_title	Custom	String
sourceUri	_source_uri	Default	String
fileType	sp_fileType	Custom	String
fileDirPath	sp_fileDirPath	Custom	String
firstPublishedDate	sp_firstPublishedDate	Custom	Date
authorId	sp_authorId	Custom	String
editorId	sp_editorId	Custom	String
category	_category	Default	String
size	sp_sizeLong	Custom	Long (numeric)

Attachments

SharePoint field name	Index field name	Description	Data type
title	sp__title	Custom	String
parentCreatedDate	_created_at	Default	Date
sourceUri	_source_uri	Default	String
parentModifiedDate	_last_updated_at	Custom	Date
parentListId	sp_parentListId	Custom	String
parentTitle	sp_parentTitle	Custom	String
category	_category	Default	String

Comments

SharePoint field name	Index field name	Description	Data type
createdDateTime	_created_at	Default	Date
likedBy	sp_likedBy	Custom	String
sourceUri	_source_uri	Custom	String
isReply	sp_isReply	Custom	String
author	_authors	Default	String list
listId	sp_listId	Custom	String
category	_category	Default	String
replyCount	sp_replyCount	Custom	String
parentTitle	sp_parentTitle	Custom	String

IAM role for Amazon Q Business SharePoint Server (Subscription Edition) connector

> **Note**
>
> **(Optional)** If you use **Azure App-Only authentication**, you also need to add permissions for Amazon Q to access the certificate stored in your Amazon S3 bucket.

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- Permission to access the SSL certificate stored in your Amazon S3 bucket.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
    "Version": "2012-10-17",       ,
    "Statement": [{
            "Sid": "AllowsAmazonQToGetS3Objects",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{input_bucket_name}}/*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{account_id}}"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToGetSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
            ]
        },
        {
```

```
            "Sid": "AllowsAmazonQToDecryptSecret",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "secretsmanager.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToIngestDocuments",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument",
                "qbusiness:BatchDeleteDocument"
            ],
            "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
        ]
        },
        {
            "Sid": "AllowsAmazonQToIngestPrincipalMapping",
            "Effect": "Allow",
            "Action": [
                "qbusiness:PutGroup",
                "qbusiness:CreateUser",
                "qbusiness:DeleteGroup",
                "qbusiness:UpdateUser",
                "qbusiness:ListGroups"
            ],
            "Resource": [
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}",
```

```
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}",
                "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}/index/{{index_id}}/data-source/*"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNI",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
                "arn:aws:ec2:{{region}}:{{account_id}}:security-group/
[[security_group]]"
            ]
        },
        {
            "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AMAZON_Q"
                    ]
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
```

```
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterfacePermission"
            ],
            "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AMAZON_Q":
 "qbusiness_{{account_id}}_{{application_id}}_*"
                }
            }
        },
        {
            "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
```

```
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the SharePoint Server (Subscription Edition) connector

The following table provides information about error codes you may see for the Microsoft SharePoint connector and suggested resolutions.

Error code	Error message	Suggested resolution
SPE-5001	Authentication failed. Configuration might contain wrong credentia ls.	Provide valid credentials like username, password or client Id, client secret and tenant Id.
SPE-5002	There was a problem while connecting to Host Url and/or Domain. hostUrl and/or domain	Provide valid Host URL or Domain.

Error code	Error message	Suggested resolution
	values might be incorrect .	
SPE-5003	Provided URL is incorrect	Provide correct URL.
SPE-5004	Inet Address validation Failed.	Provide valid Inet Address
SPE-5005	Failed : HTTP protocol violation has occurred.	Try running the connector again.
SPE-5006	Cannot connect to proxy. Check the proxy configurations.	Provide valid Proxy configuration details.
SPE-5007	Proxy port is invalid. Check the proxy port.	Provide valid Proxy port.
SPE-5008	Valid SSL Certificate could not be found for connector.	Provide valid SSL certificate.
SPE-5009	There was a problem while connecting to LDAP. Check LDAP configuration.	Provide valid LDAP configuration details.
SPE-5100	There was a problem while retrieving repositor yId. Repository ID might be empty or null.	Ensure that repository Id must not be null or empty.

Error code	Error message	Suggested resolution
SPE-5101	There was a problem while retrieving dataSourceIamRoleArn. Data Source IAM Role ARN might be empty or null.	Ensure that dataSourceIamRoleArn must not be null or empty.
SPE-5102	There was a problem while retrieving repository configurations. Repository configurations might be empty or incorrect.	Provide valid repository configurations.
SPE-5115	There was a problem while retrieving field mapping values for event entity. Field mapping values might be empty or incorrect.	Field mapping values for event entity should be correct or non-empty.
SPE-5116	There was a problem while retrieving field mapping values for file entity. Field mapping values might be empty or incorrect.	Field mapping values for file entity should be correct or non-empty.
SPE-5117	There was a problem while retrieving field mapping values for page entity. Field mapping values might be empty or incorrect.	Field mapping values for page entity should be correct or non-empty.

Error code	Error message	Suggested resolution
SPE-5118	There was a problem while retrieving field mapping values for link entity. Field mapping values might be empty or incorrect.	Field mapping values for link entity should be correct or non-empty.
SPE-5119	There was a problem while retrieving field mapping values for comment entity. Field mapping values might be empty or incorrect.	Field mapping values for comment entity should be correct or non-empty.
SPE-5120	There was a problem while retrieving field mapping values for attachment entity. Field mapping values might be empty or incorrect.	Field mapping values for attachment entity should be correct or non-empty.
SPE-5121	There was a problem while retrieving values for crawl entities. Values might be empty or incorrect. It should be either true or false.	There might be some incorrect value given in any one of the crawling entities like – null, TRUE or any dummy string. Ensure the value must be non-empty and either true or false.
SPE-5122	There was a problem while retrieving domain. Domain might be empty or null.	Provide Client Id.

Error code	Error message	Suggested resolution
SPE-5123	There was a problem while retrieving version. Version might be empty or null.	Provide valid version and it should not be null.
SPE-5124	There was a problem while retrieving authType. Auth-Type might be empty or null.	Ensure AUTH Type in configuration must be not null.
SPE-5125	There was a problem while retrieving clientId. Client ID might be empty or null.	Provide Client Id.
SPE-5126	There was a problem while retrieving clientSecret. Client Secret might be empty or null.	Provide Client Secret.
SPE-5127	There was a problem while retrieving tenantId. Tenant ID might be empty or null.	Provide Tenant Id.
SPE-5128	There was a problem while retrieving siteUrls. Site URLs might be empty or null.	Provide at least one Site Url.
SPE-5129	There was a problem while retrieving password. Password might be empty or null.	Provide password.

Error code	Error message	Suggested resolution
SPE-5130	There was a problem while retrieving username.Username might be empty or null.	Provide username.
SPE-5131	There was a problem while retrieving username. Email was invalid.	Provide valid email address.
SPE-5132	There was a problem while retrieving url. This URL was invalid.	Provide a valid URL.
SPE-5133	There was a problem while retrieving s3CertificateName. S3 Certificate Name might be empty or null.	Ensure s3CertificateName is not null or non-empty.
SPE-5134	There was a problem while retrieving s3BucketName. S3 Bucket Name might be empty or null	Ensure s3BucketName is not null or non-empty.
SPE-5135	The provided version was not a valid Sharepoint Connector version. Version should be one of [Online, Server].	Version should be one of [Online, Server].
SPE-5136	The provided authType was not a valid Sharepoint Connector authentication method.	Provide valid authType. The value of authType should be one of [Basic, OAuth2Certificate, OAuth2].

Error code	Error message	Suggested resolution
SPE-5138	There was a problem while retrieving onPremVersion. On prem Version might be empty or null	Ensure onPremVersion is not be null or non-empty.
SPE-5139	The provided onPremVersion was not valid Sharepoint on-prem version. On prem version should be one of [2013, 2016, 2019, SubscriptionEdition].	Provide a valid onPremVersion. On prem version should be one of [2013, 2016, 2019, SubscriptionEdition].
SPE-5140	There was a problem while retrieving ldapUrl. LDAP Url might be empty or null.	Ensure ldapUrl is not null or empty.
SPE-5141	There was a problem while retrieving baseDn. Base DN might be empty or null.	Ensure baseDn is not be null or empty.
SPE-5142	There was a problem while retrieving privateKey. Private Key might be empty or null.	Please ensure privateKey is not be null or empty.
SPE-5144	There was a problem while retrieving aclConfiguration. ACL Configuration might be empty, null or invalid	Provide valid aclConfiguration. aclConfiguration should be one of [ACLWithLDAPEmailFmt, ACLWithManualEmailFmt, ACLWithUsernameFmt].

Error code	Error message	Suggested resolution
SPE-5145	There was a problem while retrieving emailDomain. Email Domain might be empty or null.	Ensure emailDomain is not null or empty.
SPE-5146	There was a problem while retrieving ldapUsername. LDAP Username might be empty or null.	Ensure ldapUser is not null or empty.
SPE-5147	There was a problem while retrieving ldapPassword. LDAP Password might be empty or null.	Ensure ldapPassword is not null or empty.
SPE-5149	The provided siteUrls contain duplicate sites. Remove duplicates.	Ensure SiteUrls must not be the same.
SPE-5150	Invalid Client Id pattern.	Provide the correct client ID.
SPE-5151	Error parsing the field value. Size is over maximum allowed limit.	Ensure the size limit.
SPE-5152	There was a problem while retrieving AD Client ID. AD Client ID should not be empty.	Ensure AD Client Id must be non-empty .
SPE-5153	Invalid AD Client Id pattern.	Provide valid AD Client Id pattern.

Error code	Error message	Suggested resolution
SPE-5154	There was a problem while retrieving AD Client Secret. AD Client Secret should not be empty.	Ensure AD Client Secret is non-empty.
SPE-5155	There can't be more than one site for SharePoin t on-prem app-only authentication.	Ensure that their must be only single site present for SharePoint on-prem app-only authentication.
SPE-5200	There was a problem while connecting to the URL.	Ensure the siteUrl exists.

Connecting Microsoft Teams to Amazon Q Business

You can connect Microsoft Teams to Amazon Q Business to index and search your team's messages, channel posts, and files. This connection enables your organization to find relevant information from Teams conversations and shared content through your Amazon Q web experience.

Use the AWS Management Console or the CreateDataSource API to create the connection.

Topics

- Microsoft Teams connector versions
- Known limitations for the Microsoft Teams connector
- Microsoft Teams connector overview
- Prerequisites for connecting Amazon Q Business to Microsoft Teams
- Connecting using the latest Microsoft Teams connector (Console)
- Connecting using the legacy Microsoft Teams connector (Console)
- Connecting Amazon Q Business to Microsoft Teams using APIs
- Connecting Amazon Q Business to Microsoft Teams using AWS CloudFormation
- How Amazon Q Business connector crawls Microsoft Teams ACLs
- Microsoft Teams data source connector field mappings

- IAM role for Microsoft Teams connector
- Troubleshooting your Microsoft Teams connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Microsoft Teams connector versions

You can choose between two Microsoft Teams connector versions:

Latest Microsoft Teams connector (recommended)

> **Note**
>
> The latest connector provides improved accuracy. We recommend using the latest connector for new implementations. The legacy connector remains available if you need specific features not yet supported in the latest connector.

The latest Microsoft Teams connector offers a simplified configuration experience with the following features:

- Chat messages and channel posts syncing
- Simplified sync scope without channel wiki
- Date range filters only
- Enhanced UI layout with improved spacing
- Application-level permissions for enhanced security
- Automatic crawling of ACL and identity information

Legacy Microsoft Teams connector

The legacy Microsoft Teams connector provides full-featured configuration with advanced options:

- Complete sync scope including calendar meetings, channel wiki, and attachments
- Advanced filtering options with team names, channel names, and attachment sections
- Custom field mappings for metadata extraction
- Configurable sync modes and VPC settings
- Regex pattern matching for complex attachment filtering
- Manual ACL and identity crawling configuration

Known limitations for the Microsoft Teams connector

> **Note**
>
> **Original version notice:** We recommend using the new connector for improved performance and retrieval quality. The following limitations apply only to the original connector version.

When you use the test data source connection feature, the Microsoft Teams connector has a potential issue when testing Identity Crawler. If testing takes longer than five minutes, Amazon Q skips testing Identity Crawler and moves on to the next test. A connection error with Identity Crawler is possible even after finishing connection testing.

The Microsoft Teams connector has these known limitations:

- When you enable Access Control Lists (ACLs), the "Sync only new or modified content" option is not available due to Microsoft Teams API limitations. Use "Full sync" or "New, modified, or deleted content sync" modes instead, or disable ACLs to use this sync mode.

Microsoft Teams connector overview

The following table shows the Amazon Q Business Microsoft Teams connector features and capabilities.

Category	Feature	Latest Connector	Legacy Connector
Security	**Authentication type**	OAuth 2.0 with Client Credentials Flow	OAuth 2.0 with Client Credentials Flow
	Authentication credentials	• Microsoft Teams Client ID • Microsoft Teams Client secret	• Microsoft Teams Client ID • Microsoft Teams Client secret
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.	Yes. For more information, see ACL crawling.
	Identity crawling	Yes	Yes
	VPC	No	Yes
	Customer Managed Key (CMK) support	No	Yes
Crawl features	**Custom metadata**	No	Yes
	Entities	Chat messages, Channel posts	Yes. The following entities are supported: • Chat messages • Chat attachments • Channel posts • Channel file attachments • Wiki • Meeting chats • Meeting details • Meeting notes • Meeting files

Category	Feature	Latest Connector	Legacy Connector
			See What is a document? for more details on what each connector crawls as a document.
	Field mappings	No	Yes. Supports both default and custom field mappings. For more information, see Field mappings.

Category	Feature	Latest Connector	Legacy Connector
	Filters	Only Date range	Yes. The following filters are supported: • Include/exclude using user email • Include/exclude using team name • Include/exclude using channel name • Include/exclude using file name • Include/exclude using file type • Chat message • Chat attachment • Channel post • Channel attachment • Channel wiki • Calendar meeting • Meeting chat • Meeting file • Meeting note
	Sync mode	Full sync only	Supports full and incremental sync

Prerequisites for connecting Amazon Q Business to Microsoft Teams

Before you begin, make sure that you have completed the following prerequisites.

In Microsoft Teams, make sure you have:

- Created a Microsoft Teams account in Office 365.
- Copied your Microsoft 365 Tenant ID. You can find your Tenant ID in the Properties of your Azure Active Directory Portal. You need this URL to allow Amazon Q to connect with your Microsoft Teams data source. For more information, see Register a Microsoft Entra app and create a service principal on the Microsoft website.
- Configured an OAuth 2.0 credential token containing a client ID and client secret. For more information, see Azure documentation on managing access tokens for Teams on the Microsoft website.
- Added the necessary permissions. You can choose to add all permissions, or you can limit the scope by selecting fewer permissions based on which entities you want to crawl. *(Application level permissions required for new connector)* All permissions must be at *application* level, not delegated. The following table shows permissions by corresponding entity.

Entity	Required permissions for data sync	Required permissions for identity sync
Channel Post	• ChannelMessage.Read.All • Group.Read.All • User.Read • User.Read.All	TeamMember.Read.All
Chat Message	• Chat.Read.All • ChatMessage.Read.All • ChatMember.Read.All • User.Read • User.Read.All • Group.Read.All	TeamMember.Read.All
Calendar Meeting	• Chat.Read.All • ChatMessage.Read.All • ChatMember.Read.All • User.Read • User.Read.All • Group.Read.All	TeamMember.Read.All

Entity	Required permissions for data sync	Required permissions for identity sync
	• Files.Read.All	
Meeting Notes	• User.Read • User.Read.All • Group.Read.All • Files.Read.All	TeamMember.Read.All

- Generated Microsoft Teams OAuth 2.0 credentials containing a client ID, client secret, username, and password. You need these credentials to authenticate Amazon Q to access Microsoft Teams.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Microsoft Teams authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting using the latest Microsoft Teams connector (Console)

The latest Microsoft Teams connector provides a simplified configuration experience with essential features. Use this procedure to connect Amazon Q Business to Microsoft Teams using the latest connector.

To connect Amazon Q to Microsoft Teams using the latest connector

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Microsoft Teams** data source to your Amazon Q application.
5. Then, on the **Microsoft Teams** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, enter the following information:

   - **Tenant ID** – Enter your Tenant ID.

     > **Note**
     >
     > Your Microsoft Tenant ID is a globally unique identifier that's necessary to configure each connector instance. Your Tenant ID is different from your organization name or domain and can be found in the **Properties** section of your Azure Active Directory Portal.
8. For **Authentication**, in **AWS Secrets Manager** – Choose between **Create and add new secret** and **Use existing secrets**.

   - If you choose **Use existing secrets**, select an existing secret.

     If you choose **Create and add a new secret**, enter the following information in the **Create AWS Secrets Manager secret** section:

i. **Secret name** – A name for your secret.

ii. **Client ID** – Enter the Client ID you generated after registering your application for use. You can find this Client ID in **App registrations** in your Azure Active Directory Portal.

iii. **Client Secret** – Enter the client secret that you generated from your Teams account.

9. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

10. **Sync scope** – Choose the content you want to sync.

a. Choose **All** to crawl and sync all your documents.

b. For **Chat**, choose from the following options:

i. Choose **Chat** to crawl and sync all chats. If you choose this option, Amazon Q Business also crawls **Chat messages** by default.

ii. Choose **Chat messages** to crawl and sync only all chat messages.

c. For **Teams**, choose from the following options:

i. Choose **Teams** to crawl and sync all teams. If you choose this option, Amazon Q Business also crawls **Channel posts** by default.

ii. Choose **Channel posts** to crawl and sync only all channel posts.

d. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

11. In **Additional configuration – *optional***, configure the following simplified options:

- **Date Range** – Enter the date range for which the connector will crawl your content. End date is optional. Rolling window options available: Last [X] Days/Weeks/Months.

> **Note**
>
> **Simplified configuration:** The latest connector automatically handles entity selection with ACL enabled by default to keep the configuration simple and reliable.

12. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
13. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
14. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting using the legacy Microsoft Teams connector (Console)

The legacy Microsoft Teams connector provides comprehensive configuration options including entity type selection, field mappings, and VPC settings. Use this procedure to connect Amazon Q Business to Microsoft Teams using the legacy connector.

To connect Amazon Q to Microsoft Teams using the legacy connector

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Microsoft Teams** data source to your Amazon Q application.
5. Then, on the **Microsoft Teams** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, enter the following information:

   - **Tenant ID** – Enter your Tenant ID.

     > **Note**
     >
     > Your Microsoft Tenant ID is a globally unique identifier that's necessary to configure each connector instance. Your Tenant ID is different from your organization name or domain and can be found in the **Properties** section of your Azure Active Directory Portal.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
9. For **Authentication**, in **AWS Secrets Manager** – Choose between **Create and add new secret** and **Use existing secrets**.

- If you choose **Use existing secrets**, select an existing secret.

  If you choose **Create and add a new secret**, enter the following information in the **Create AWS Secrets Manager secret** section:

  i. **Secret name** – A name for your secret.

  ii. **Client ID** – Enter the Client ID you generated after registering your application for use. You can find this Client ID in **App registrations** in your Azure Active Directory Portal.

  iii. **Client Secret** – Enter the client secret that you generated from your Teams account.

10. **Payment model** – Choose the payment model associated with your Microsoft Teams account. Model A payment models are restricted to licensing and payment models that require security compliance. Model B payment models are suitable for licensing and payment models that don't require security compliance.
11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.
12. **Sync scope** – Choose the content you want to sync.

    a. Choose **All** to crawl and sync all your documents.

    b. For **Chat**, choose from the following options:

    i. Choose **Chat** to crawl and sync all chats. If you choose this option, Amazon Q Business also crawls **Chat messages** and **Chat files** by default.

    ii. Choose **Chat messages** to crawl and sync only all chat messages.

    iii. Choose **Chat files** to crawl and sync only all chat files.

    c. For **Teams**, choose from the following options:

i. Choose **Teams** to crawl and sync all teams. If you choose this option, Amazon Q Business also crawls **Channel posts**, **Channel files and folders** and **Channel wiki** by default.

ii. Choose **Channel posts** to crawl and sync only all channel posts.

iii. Choose **Channel files and folders** to crawl and sync only all channel files and folders.

iv. Choose **Channel wiki** to crawl and sync only all channel wikis.

d. For **Calendar**, choose from the following options:

i. Choose **Calendar** to crawl and sync your calendar. If you choose this option, Amazon Q Business also crawls **Meetings**, **Meeting chats**, **Meeting files** and **Meeting notes** by default.

ii. Choose **Meetings** to crawl and sync only all meetings.

iii. Choose **Meeting chats** to crawl and sync only all meeting chats.

iv. Choose **Meeting files** to crawl and sync only all meeting files.

v. Choose **Meeting notes** to crawl and sync only all meeting notes.

e. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

To extract audio transcriptions and video content, enable processing for the following file types:

f. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

13. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
14. In **Additional configuration – *optional***, configure the following comprehensive options:

- **Calendar crawling** – Enter the date range for which the connector will crawl your calendar content.
- **User email** – Enter the emails of the users you want to include in your application.

- **Team names** – Add patterns to include or exclude teams found in Microsoft Teams from your application.
- **Channel names** – Add patterns to include or exclude channels found in Microsoft Teams from your application.
- **Attachment regex patterns** – Add regular expression patterns to include or exclude certain attachment for all supported entities. You can add up to 100 patterns.

15. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

16. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

For more information, see VPC.

17. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
18. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Microsoft Teams using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- Connecting Amazon Q Business to Microsoft Teams (new connector) using APIs
- Connecting Amazon Q Business to Microsoft Teams (Original connector) using APIs

Connecting Amazon Q Business to Microsoft Teams (new connector) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Microsoft Teams new connector JSON schema

The following is the Microsoft Teams new connector JSON schema:

```
{
  "$schema": "https://json-schema.org/draft-07/schema#",
  "$id": "https://amazonaws.com/plato/connector/configuration/msteams",
  "title": "Microsoft Teams Configuration Schema",
  "description": "JSON Schema for Microsoft Teams data connector configuration based on
 Smithy model",
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": [
        "MSTEAMSV2"
      ],
      "description": "The connector type identifier"
    },
    "connectionConfiguration": {
      "type": "object",
      "description": "Configuration for connecting to Microsoft Teams",
      "properties": {
        "tenantId": {
          "type": "string",
          "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[4][0-9a-f]{3}-[89ab][0-9a-f]{3}-[0-9a-
f]{12}$",
          "minLength": 36,
          "maxLength": 36,
          "description": "Microsoft Teams tenant ID in UUID v4 format"
        },
        "secretArn": {
          "type": "string",
```

```
          "pattern": "^arn:[a-z0-9-\\.]{1,63}:[a-z0-9-\\.]{0,63}:[a-z0-9-\\.]{0,63}:[a-
z0-9-\\.]{0,63}:[^/].{0,1023}$",
          "description": "ARN of the AWS Secrets Manager secret containing
 authentication credentials"
        }
      },
      "required": ["tenantId", "secretArn"],
      "additionalProperties": false
    },
    "filterConfiguration": {
      "type": "object",
      "description": "Configuration for filtering data based on date ranges",
      "properties": {
        "startDateFilter": {
          "type": "string",
          "pattern": "^\\d{4}-\\d{2}-\\d{2}T\\d{2}:\\d{2}:\\d{2}(?:\\.\\d+)?(?:Z|[+-]\
\d{2}:\\d{2})$",
          "description": "Start date for filtering data in ISO 8601 format"
        },
        "endDateFilter": {
          "type": "string",
          "pattern": "^\\d{4}-\\d{2}-\\d{2}T\\d{2}:\\d{2}:\\d{2}(?:\\.\\d+)?(?:Z|[+-]\
\d{2}:\\d{2})$",
          "description": "End date for filtering data in ISO 8601 format"
        }
      },
      "additionalProperties": false
    },
    "dataEntityConfiguration": {
      "type": "object",
      "description": "Configuration for specifying which data entities to crawl",
      "properties": {
        "crawlChatMessages": {
          "type": "boolean",
          "description": "Whether to crawl chat messages from Microsoft Teams"
        },
        "crawlChannelPosts": {
          "type": "boolean",
          "description": "Whether to crawl channel posts from Microsoft Teams"
        }
      },
      "additionalProperties": false
    },
    "deletionProtectionConfiguration": {
```

```
      "type": "object",
      "description": "Configuration for deletion protection settings",
      "properties": {
        "enableDeletionProtection": {
          "type": "boolean",
          "description": "Whether to enable deletion protection"
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "pattern": "^(100|[1-9][0-9]?)$",
          "description": "Deletion protection threshold as a percentage (1-100)"
        }
      },
      "additionalProperties": false
    }
  },
  "required": [
    "type",
    "connectionConfiguration",
    "dataEntityConfiguration"
  ],
  "additionalProperties": false,
  "examples": [
    {
      "type": "MSTEAMSV2",
      "connectionConfiguration": {
        "tenantId": "12345678-1234-4123-8123-123456789012",
        "secretArn": "arn:aws:secretsmanager:us-east-1:123456789012:secret:msteams-
credentials-AbCdEf"
      },
      "filterConfiguration": {
        "startDateFilter": "2024-01-01T00:00:00Z",
        "endDateFilter": "2024-12-31T23:59:59Z"
      },
      "dataEntityConfiguration": {
        "crawlChatMessages": true,
        "crawlChannelPosts": true
      },
      "deletionProtectionConfiguration": {
        "enableDeletionProtection": true,
        "deletionProtectionThreshold": "10"
      }
    }
  ]
```

```
}
```

The following table provides information about important JSON keys to configure for the new Microsoft Teams connector.

Configuration	Description
`type`	The type of data source. Must be `MSTEAMSV2` for the new Teams connector.
`connectionConfiguration`	Configuration information for connecting to the Teams data source.
`tenantId`	The Microsoft Teams tenant ID in UUID v4 format.
`secretArn`	The Amazon Resource Name (ARN) of a Secrets Manager secret that contains the key-value pairs required to connect to your Microsoft Teams.
`dataEntityConfiguration`	Configuration for the types of data entities to crawl from Teams.
`crawlChatMessages`	A Boolean value to specify whether to crawl chat messages. Set to `true` to include chat messages in the crawl, or `false` to exclude them.
`crawlChannelPosts`	A Boolean value to specify whether to crawl channel posts. Set to `true` to include channel posts in the crawl, or `false` to exclude them.
`filterConfiguration`	Optional configuration for filtering content during the crawl process.
`startDateFilter`	Specify the start date for filtering content. Only content created on or after this date

Configuration	Description
	will be crawled. Format: ISO 8601 date-time format.
`endDateFilter`	Specify the end date for filtering content. Only content created on or before this date will be crawled. Format: ISO 8601 date-time format.
`deletionProtectionConfiguration`	Optional configuration to protect against accidental deletion of large amounts of content.
`enableDeletionProtection`	A Boolean value to enable deletion protectio n. When enabled, the connector will not delete more than the specified threshold of documents in a single sync.
`deletionProtectionThreshold`	The maximum percentage of documents that can be deleted in a single sync when deletion protection is enabled. Specify as a string containing a number from 1 to 100.

Connecting Amazon Q Business to Microsoft Teams (Original connector) using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Microsoft Teams configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for endpoint for the data source.	`object` This property has the following sub-property: `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-property: `tenantId`.	Yes
`tenantId`	The Microsoft 365 tenant ID. You can find your tenant ID in the Properties of your Azure Active Directory Portal.	`string` The string must be 36 characters long and in in the pattern: ^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$	Yes
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties: • `chatMessage` • `chatAttachment` • `channelPost` • `channelWiki` • `channelAttachment`	Yes

Configuration	Description	Type	Required
		• `meetingChat` • `meetingFile` • `meetingNote` • `calendarMeeting`	
• `chatMessage` • `chatAttachment` • `channelPost` • `channelWiki` • `channelAttachment` • `meetingChat` • `meetingFile` • `meetingNote` • `calendarMeeting`	A list of objects that map the attributes or field names of your Microsoft Teams content to Amazon Q index field names.	`object` These properties have the following sub-properties: `indexFieldName` , `indexFieldType` , `dataSourceFieldName` , and `dateFieldFormat` .	No
`indexFieldName`	The field name of your Microsoft Teams assets.	`string`	Yes
`indexFieldType`	The field type of your Microsoft Teams assets.	`string` The allowed values are `STRING`, `STRING_LIST` , `DATE`, and `LONG`.	Yes
`dataSourceFieldName`	The data source field name of your Microsoft Teams assets.	`string`	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The date format of your Microsoft Teams assets.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties. • isCrawlAcl • isCrawlChatMessage • isCrawlChatAttachment • isCrawlChannelPost • isCrawlChannelAttachment • isCrawlChannelWiki • isCrawlCalendarMeeting • isCrawlMeetingChat • isCrawlMeetingFile • isCrawlMeetingNote • startCalendarDateTime • endCalendarDateTime	Yes

Configuration	Description	Type	Required
		• fieldForUserId • paymentModel • maxFileSizeInMegaBytes • inclusionTeamNameFilter • exclusionTeamNameFilter • inclusionChannelNameFilter • exclusionChannelNameFilter • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionFileTypePatterns • exclusionFileTypePatterns	

Configuration	Description	Type	Required
		• `inclusionUserEmailFilter`	
`isCrawlAcl`	Specify `true` to crawl access control information from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.	`boolean`	No

Configuration	Description	Type	Required
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string`	No
`fieldForUserId`	Specify the field to use for `UserId` for ACL crawling.	`string`	No

Configuration	Description	Type	Required
• `isCrawlChatMessage` • `isCrawlChatAttachment` • `isCrawlChannelPost` • `isCrawlChannelAttachment` • `isCrawlChannelWiki` • `isCrawlCalendarMeeting` • `isCrawlMeetingChat` • `isCrawlMeetingFile` • `isCrawlMeetingNote`	Specify `true` to index this content in your Microsoft Teams data source.	`boolean`	No

Configuration	Description	Type	Required
• `inclusionTeamNameFilter` • `inclusionChannelNameFilter` • `inclusionFileNamePatterns` • `inclusionFileTypePatterns` • `inclusionUserEmailFilter`	A list of regular expression patterns to include specific content in your Microsoft Teams data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array (string)`	No

Configuration	Description	Type	Required
• exclusionTeamNameFilter • exclusionChannelNameFilter • exclusionFileNamePatterns • exclusionFileTypePatterns	A list of regular expression patterns to exclude specific content in your Microsoft Teams data source. Content that matches the patterns are excluded from the index. Content that doesn't match the patterns are included in the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	array (string)	No
• startCalendarDateTime • endCalendarDateTime	You can choose to configure a startCalendarDateTime and endCalendarDateTime parameters so that the Microsoft Teams connector crawls content based on a specific date range.	string Specify the date in the form ^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$)	No

Configuration	Description	Type	Required
`paymentModel`	Specifies what type of payment model to use with your Teams data source. Model A payment models are restricted to licensing and payment models that require security compliance. Model B payment models are suitable for licensing and payment models that don't require security compliance.	`string` Valid values are A, B, and `Evaluation Mode`.	No

Configuration	Description	Type	Required
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	`string` You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required

`secretARN`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Microsoft Teams.	`string`
		
		The secret must contain a JSON structure with the following keys:
		
		`{ "clientId": String, "clientSecret": String }`
			Yes

`type`	The type of data source. Specify `MSTEAMS` as your data source type.	`string`	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler.Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information,	`boolean`	No

Configuration	Description	Type	Required
	see Identity crawler.		
`version`	The version of this template that's currently supported.	`string`	No

Microsoft Teams JSON schema

The following is the Microsoft Teams JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "pattern": "MSTEAMS"
    },
    "syncMode": {
      "type": "string",
      "enum": ["FORCED_FULL_CRAWL", "FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
```

```
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            }
          },
          "required": ["tenantId"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "chatMessage": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
```

```
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "chatAttachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
```

```
          },
          "required": ["fieldMappings"]
        },
        "channelPost": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "channelWiki": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
```

```
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "channelAttachment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "DATE", "LONG"]
```

```
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "meetingChat": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
```

```
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "meetingFile": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
```

```
          "required": ["fieldMappings"]
        },
        "meetingNote": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "calendarMeeting": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
```

```
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "isCrawlAcl": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
```

```
        "maxFileSizeInMegaBytes": {
          "type": "string"
        },
        "fieldForUserId": {
          "type": "string"
        },
        "paymentModel": {
          "type": "string",
          "enum": ["A", "B", "Evaluation Mode"]
        },
        "inclusionTeamNameFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionTeamNameFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionChannelNameFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionChannelNameFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
```

```
        }
      },
      "inclusionFileTypePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionFileTypePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionUserEmailFilter": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "isCrawlChatMessage": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlChatAttachment": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlChannelPost": {
        "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlChannelAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlChannelWiki": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlCalendarMeeting": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlMeetingChat": {
          "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlMeetingFile": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlMeetingNote": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "startCalendarDateTime": {
          "anyOf": [
            {
              "type": "string",
              "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
            },
            {
              "type": "string",
              "pattern": ""
            }
          ]
        },
        "endCalendarDateTime": {
```

```
          "anyOf": [
            {
              "type": "string",
              "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
            },
            {
              "type": "string",
              "pattern": ""
            }
          ]
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    },
    "required": [
      "type",
      "syncMode",
      "secretArn",
      "connectionConfiguration",
      "repositoryConfigurations",
```

```
      "additionalProperties"
    ]
  }
}
```

Microsoft Teams JSON schema example

The following is the Microsoft Teams JSON schema example:

```
{
  "type": "MSTEAMS",
  "syncMode": "FULL_CRAWL",
  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-teams-secret",
  "enableIdentityCrawler": "true",
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "tenantId": "123e4567-e89b-12d3-a456-426614174000"
    }
  },
  "repositoryConfigurations": {
    "chatMessage": {
      "fieldMappings": [
        {
          "indexFieldName": "message_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "chatAttachment": {
      "fieldMappings": [
        {
          "indexFieldName": "attachment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "channelPost": {
      "fieldMappings": [
        {
          "indexFieldName": "post_id",
```

```
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "channelWiki": {
      "fieldMappings": [
        {
          "indexFieldName": "wiki_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "channelAttachment": {
      "fieldMappings": [
        {
          "indexFieldName": "attachment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "meetingChat": {
      "fieldMappings": [
        {
          "indexFieldName": "meeting_chat_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "meetingFile": {
      "fieldMappings": [
        {
          "indexFieldName": "meeting_file_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
```

```
      ]
    },
    "meetingNote": {
      "fieldMappings": [
        {
          "indexFieldName": "meeting_note_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "calendarMeeting": {
      "fieldMappings": [
        {
          "indexFieldName": "calendar_meeting_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    }
  },
  "additionalProperties": {
    "isCrawlAcl": "true",
    "maxFileSizeInMegaBytes": "50",
    "fieldForUserId": "user_id",
    "paymentModel": "A",
    "inclusionTeamNameFilter": ["TeamA", "TeamB"],
    "exclusionTeamNameFilter": ["TeamC"],
    "inclusionChannelNameFilter": ["Channel1", "Channel2"],
    "exclusionChannelNameFilter": ["Channel3"],
    "inclusionFileNamePatterns": ["*.docx", "*.pdf"],
    "exclusionFileNamePatterns": ["*.tmp"],
    "inclusionFileTypePatterns": ["image/png", "image/jpeg"],
    "exclusionFileTypePatterns": ["application/octet-stream"],
    "inclusionUserEmailFilter": ["user@example.com"],
    "isCrawlChatMessage": "true",
    "isCrawlChatAttachment": "true",
    "isCrawlChannelPost": "true",
    "isCrawlChannelAttachment": "true",
    "isCrawlChannelWiki": "true",
    "isCrawlCalendarMeeting": "true",
    "isCrawlMeetingChat": "true",
```

```
    "isCrawlMeetingFile": "true",
    "isCrawlMeetingNote": "true",
    "startCalendarDateTime": "2023-01-01T00:00:00Z",
    "endCalendarDateTime": "2023-12-31T23:59:59Z",
    "enableDeletionProtection": "false",
    "deletionProtectionThreshold": "15"
  }
}
```

Connecting Amazon Q Business to Microsoft Teams using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Microsoft Teams configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for endpoint for the data source.	`object` This property has the following sub-property: `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-property: `tenantId`.	Yes

Configuration	Description	Type	Required
`tenantId`	The Microsoft 365 tenant ID. You can find your tenant ID in the Properties of your Azure Active Directory Portal.	`string` The string must be 36 characters long and in in the pattern: ^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$	Yes
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-properties: • `chatMessage` • `chatAttachment` • `channelPost` • `channelWiki` • `channelAttachment` • `meetingChat` • `meetingFile` • `meetingNote` • `calendarMeeting`	Yes

Configuration	Description	Type	Required
• chatMessage • chatAttachment • channelPost • channelWiki • channelAttachment • meetingChat • meetingFile • meetingNote • calendarMeeting	A list of objects that map the attributes or field names of your Microsoft Teams content to Amazon Q index field names.	object These properties have the following sub-properties: indexFieldName , indexFieldType , dataSourceFieldName , and dateFieldFormat .	No
indexFieldName	The field name of your Microsoft Teams assets.	string	Yes
indexFieldType	The field type of your Microsoft Teams assets.	string The allowed values are STRING, STRING_LIST , DATE, and LONG.	Yes
dataSourceFieldName	The data source field name of your Microsoft Teams assets.	string	Yes

Configuration	Description	Type	Required
`dateFieldFormat`	The date format of your Microsoft Teams assets.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties. • isCrawlAcl • isCrawlChatMessage • isCrawlChatAttachment • isCrawlChannelPost • isCrawlChannelAttachment • isCrawlChannelWiki • isCrawlCalendarMeeting • isCrawlMeetingChat • isCrawlMeetingFile • isCrawlMeetingNote • startCalendarDateTime • endCalendarDateTime	Yes

Configuration	Description	Type	Required
		• fieldForUserId • paymentModel • maxFileSizeInMegaBytes • inclusionTeamNameFilter • exclusionTeamNameFilter • inclusionChannelNameFilter • exclusionChannelNameFilter • inclusionFileNamePatterns • exclusionFileNamePatterns • inclusionFileTypePatterns • exclusionFileTypePatterns	

Configuration	Description	Type	Required
		• `inclusionUserEmailFilter`	
`isCrawlAcl`	Specify `true` to crawl access control information from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.	`boolean`	No

Configuration	Description	Type	Required
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string`	No
`fieldForUserId`	Specify the field to use for `UserId` for ACL crawling.	`string`	No

Configuration	Description	Type	Required
• isCrawlChatMessage • isCrawlChatAttachment • isCrawlChannelPost • isCrawlChannelAttachment • isCrawlChannelWiki • isCrawlCalendarMeeting • isCrawlMeetingChat • isCrawlMeetingFile • isCrawlMeetingNote	Specify `true` to index this content in your Microsoft Teams data source.	`boolean`	No

Configuration	Description	Type	Required
• `inclusionTeamNameFilter` • `inclusionChannelNameFilter` • `inclusionFileNamePatterns` • `inclusionFileTypePatterns` • `inclusionUserEmailFilter`	A list of regular expression patterns to include specific content in your Microsoft Teams data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array (string)`	No

Configuration	Description	Type	Required
• exclusionTeamNameFilter • exclusionChannelNameFilter • exclusionFileNamePatterns • exclusionFileTypePatterns	A list of regular expression patterns to exclude specific content in your Microsoft Teams data source. Content that matches the patterns are excluded from the index. Content that doesn't match the patterns are included in the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	array (string)	No
• startCalendarDateTime • endCalendarDateTime	You can choose to configure a startCalendarDateTime and endCalendarDateTime parameters so that the Microsoft Teams connector crawls content based on a specific date range.	string Specify the date in the form ^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$)	No

Configuration	Description	Type	Required
`paymentModel`	Specifies what type of payment model to use with your Teams data source. Model A payment models are restricted to licensing and payment models that require security compliance. Model B payment models are suitable for licensing and payment models that don't require security compliance.	`string` Valid values are A, B, and `Evaluation Mode`.	No

Configuration	Description	Type	Required
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	`string` You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required

secretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Microsoft Teams.	string
		
		The secret must contain a JSON structure with the following keys:
		
		{
		"clientId": String,
		"clientSecret": String
		}
			Yes

type	The type of data source. Specify MSTEAMS as your data source type.	string	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler.Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information,	`boolean`	No

Configuration	Description	Type	Required
	see Identity crawler.		
`version`	The version of this template that's currently supported.	`string`	No

Microsoft Teams JSON schema for using the CloudFormation

Microsoft Teams JSON schema for using the CloudFormation

The following is the Microsoft Teams JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- Microsoft Teams JSON schema for using the configuration property with AWS CloudFormation
- Microsoft Teams JSON schema example for using the configuration property with AWS CloudFormation

Microsoft Teams JSON schema for using the configuration property with AWS CloudFormation

The following is the Microsoft Teams JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "pattern": "MSTEAMS"
    },
    "syncMode": {
      "type": "string",
      "enum": ["FORCED_FULL_CRAWL", "FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string",
```

```
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            }
          },
          "required": ["tenantId"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "chatMessage": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
```

```
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "chatAttachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
```

```
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "channelPost": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
```

```
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "channelWiki": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
```

```
        "channelAttachment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "meetingChat": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
```

```
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "meetingFile": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
```

```
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "meetingNote": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
```

```
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "calendarMeeting": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        }
      }
```

```
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "isCrawlAcl": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "maxFileSizeInMegaBytes": {
          "type": "string"
        },
        "fieldForUserId": {
          "type": "string"
        },
        "paymentModel": {
          "type": "string",
          "enum": ["A", "B", "Evaluation Mode"]
        },
        "inclusionTeamNameFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionTeamNameFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionChannelNameFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionChannelNameFilter": {
```

```
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionUserEmailFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "isCrawlChatMessage": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
```

```
          ]
        },
        "isCrawlChatAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlChannelPost": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlChannelAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlChannelWiki": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
```

```
          ]
        },
        "isCrawlCalendarMeeting": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlMeetingChat": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlMeetingFile": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlMeetingNote": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
```

```
          ]
        },
        "startCalendarDateTime": {
          "anyOf": [
            {
              "type": "string",
              "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
            },
            {
              "type": "string",
              "pattern": ""
            }
          ]
        },
        "endCalendarDateTime": {
          "anyOf": [
            {
              "type": "string",
              "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
            },
            {
              "type": "string",
              "pattern": ""
            }
          ]
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
```

```
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    },
    "required": [
      "type",
      "syncMode",
      "secretArn",
      "connectionConfiguration",
      "repositoryConfigurations",
      "additionalProperties"
    ]
  }
}
```

Microsoft Teams JSON schema example for using the configuration property with AWS CloudFormation

The following is the Microsoft Teams JSON schema example for the configuration property for CloudFormation

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation MSTEAMS Data Source Template",
  "Resources": {
    "DataSourceMSTeams": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MyMSTeamsDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "MSTEAMS",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-teams-
secret",
          "enableIdentityCrawler": "true",
```

```
        "connectionConfiguration": {
          "repositoryEndpointMetadata": {
            "tenantId": "123e4567-e89b-12d3-a456-426614174000"
          }
        },
        "repositoryConfigurations": {
          "chatMessage": {
            "fieldMappings": [
              {
                "indexFieldName": "message_id",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          },
          "chatAttachment": {
            "fieldMappings": [
              {
                "indexFieldName": "attachment_id",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          },
          "channelPost": {
            "fieldMappings": [
              {
                "indexFieldName": "post_id",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          },
          "channelWiki": {
            "fieldMappings": [
              {
                "indexFieldName": "wiki_id",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
```

```
            ]
          },
          "channelAttachment": {
            "fieldMappings": [
              {
                "indexFieldName": "attachment_id",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          },
          "meetingChat": {
            "fieldMappings": [
              {
                "indexFieldName": "meeting_chat_id",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          },
          "meetingFile": {
            "fieldMappings": [
              {
                "indexFieldName": "meeting_file_id",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          },
          "meetingNote": {
            "fieldMappings": [
              {
                "indexFieldName": "meeting_note_id",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          },
          "calendarMeeting": {
            "fieldMappings": [
```

```
                {
                  "indexFieldName": "calendar_meeting_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
            }
          },
          "additionalProperties": {
            "isCrawlAcl": "true",
            "maxFileSizeInMegaBytes": "50",
            "fieldForUserId": "user_id",
            "paymentModel": "A",
            "inclusionTeamNameFilter": ["TeamA", "TeamB"],
            "exclusionTeamNameFilter": ["TeamC"],
            "inclusionChannelNameFilter": ["Channel1", "Channel2"],
            "exclusionChannelNameFilter": ["Channel3"],
            "inclusionFileNamePatterns": ["*.docx", "*.pdf"],
            "exclusionFileNamePatterns": ["*.tmp"],
            "inclusionFileTypePatterns": ["image/png", "image/jpeg"],
            "exclusionFileTypePatterns": ["application/octet-stream"],
            "inclusionUserEmailFilter": ["user@example.com"],
            "isCrawlChatMessage": "true",
            "isCrawlChatAttachment": "true",
            "isCrawlChannelPost": "true",
            "isCrawlChannelAttachment": "true",
            "isCrawlChannelWiki": "true",
            "isCrawlCalendarMeeting": "true",
            "isCrawlMeetingChat": "true",
            "isCrawlMeetingFile": "true",
            "isCrawlMeetingNote": "true",
            "startCalendarDateTime": "2023-01-01T00:00:00Z",
            "endCalendarDateTime": "2023-12-31T23:59:59Z",
            "enableDeletionProtection": "false",
            "deletionProtectionThreshold": "15"
          }
        }
      }
    }
  }
}
```

Microsoft Teams YAML schema for using the configuration property with AWS CloudFormation

The following is the Microsoft Teams YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- Microsoft Teams YAML schema for using the configuration property with AWS CloudFormation
- Microsoft Teams YAML schema example for using the configuration property with AWS CloudFormation

Microsoft Teams YAML schema for using the configuration property with AWS CloudFormation

The following is the Microsoft Teams YAML schema for the configuration property for CloudFormation.

```
type: object
properties:
  type:
    type: string
    pattern: MSTEAMS
  syncMode:
    type: string
    enum:
      - FORCED_FULL_CRAWL
      - FULL_CRAWL
      - CHANGE_LOG
  secretArn:
    type: string
    minLength: 20
    maxLength: 2048
  enableIdentityCrawler:
    anyOf:
      - type: boolean
      - type: string
        enum:
          - "true"
          - "false"
  connectionConfiguration:
    type: object
    properties:
      repositoryEndpointMetadata:
        type: object
```

```
        properties:
          tenantId:
            type: string
            pattern: "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$"
            minLength: 36
            maxLength: 36
        required:
          - tenantId
    required:
      - repositoryEndpointMetadata
  repositoryConfigurations:
    type: object
    properties:
      chatMessage:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      chatAttachment:
        type: object
        properties:
          fieldMappings:
```

```
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - DATE
                    - LONG
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      channelPost:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
```

```
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
        required:
          - fieldMappings
      channelWiki:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - DATE
                    - LONG
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      channelAttachment:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
```

```
                type: string
                enum:
                  - STRING
                  - DATE
                  - LONG
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
        required:
          - fieldMappings
      meetingChat:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      meetingFile:
```

```
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - DATE
                    - LONG
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
        required:
          - fieldMappings
      meetingNote:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
```

```
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
        required:
          - fieldMappings
      calendarMeeting:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - DATE
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
  additionalProperties:
    type: object
    properties:
      isCrawlAcl:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
```

```
      maxFileSizeInMegaBytes:
        type: string
      fieldForUserId:
        type: string
      paymentModel:
        type: string
        enum:
          - A
          - B
          - Evaluation Mode
      inclusionTeamNameFilter:
        type: array
        items:
          type: string
      exclusionTeamNameFilter:
        type: array
        items:
          type: string
      inclusionChannelNameFilter:
        type: array
        items:
          type: string
      exclusionChannelNameFilter:
        type: array
        items:
          type: string
      inclusionFileNamePatterns:
        type: array
        items:
          type: string
      exclusionFileNamePatterns:
        type: array
        items:
          type: string
      inclusionFileTypePatterns:
        type: array
        items:
          type: string
      exclusionFileTypePatterns:
        type: array
        items:
          type: string
      inclusionUserEmailFilter:
        type: array
```

```
        items:
          type: string
      isCrawlChatMessage:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      isCrawlChatAttachment:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      isCrawlChannelPost:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      isCrawlChannelAttachment:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      isCrawlChannelWiki:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      isCrawlCalendarMeeting:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
```

```
      isCrawlMeetingChat:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      isCrawlMeetingFile:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      isCrawlMeetingNote:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      startCalendarDateTime:
        anyOf:
          - type: string
            pattern: "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
          - type: string
            pattern: ""
      endCalendarDateTime:
        anyOf:
          - type: string
            pattern: "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
          - type: string
            pattern: ""
      enableDeletionProtection:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
        default: false
      deletionProtectionThreshold:
        type: string
        default: "15"
```

```
    required: []
  version:
    type: string
    anyOf:
      - pattern: "1.0.0"
  required:
    - connectionConfiguration
    - repositoryConfigurations
    - syncMode
    - additionalProperties
    - secretArn
    - type
```

Microsoft Teams YAML schema example for using the configuration property with AWS CloudFormation

The following is the Microsoft Teams YAML example for the Configuration property for CloudFormation:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: CloudFormation MSTEAMS Data Source Template
Resources:
  DataSourceMSTeams:
    Type: AWS::QBusiness::DataSource
    Properties:
      ApplicationId: app12345-1234-1234-1234-123456789012
      IndexId: indx1234-1234-1234-1234-123456789012
      DisplayName: MyMSTeamsDataSource
      RoleArn: arn:aws:iam::123456789012:role/qbusiness-data-source-role
      Configuration:
        type: MSTEAMS
        syncMode: FULL_CRAWL
        secretArn: arn:aws:secretsmanager:us-west-2:123456789012:secret:my-teams-secret
        enableIdentityCrawler: "true"
        connectionConfiguration:
          repositoryEndpointMetadata:
            tenantId: 123e4567-e89b-12d3-a456-426614174000
        repositoryConfigurations:
          chatMessage:
            fieldMappings:
              - indexFieldName: message_id
                indexFieldType: STRING
                dataSourceFieldName: id
```

```
      dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
  chatAttachment:
    fieldMappings:
      - indexFieldName: attachment_id
        indexFieldType: STRING
        dataSourceFieldName: id
        dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
  channelPost:
    fieldMappings:
      - indexFieldName: post_id
        indexFieldType: STRING
        dataSourceFieldName: id
        dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
  channelWiki:
    fieldMappings:
      - indexFieldName: wiki_id
        indexFieldType: STRING
        dataSourceFieldName: id
        dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
  channelAttachment:
    fieldMappings:
      - indexFieldName: attachment_id
        indexFieldType: STRING
        dataSourceFieldName: id
        dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
  meetingChat:
    fieldMappings:
      - indexFieldName: meeting_chat_id
        indexFieldType: STRING
        dataSourceFieldName: id
        dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
  meetingFile:
    fieldMappings:
      - indexFieldName: meeting_file_id
        indexFieldType: STRING
        dataSourceFieldName: id
        dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
  meetingNote:
    fieldMappings:
      - indexFieldName: meeting_note_id
        indexFieldType: STRING
        dataSourceFieldName: id
        dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
  calendarMeeting:
```

```
        fieldMappings:
          - indexFieldName: calendar_meeting_id
            indexFieldType: STRING
            dataSourceFieldName: id
            dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
      additionalProperties:
        isCrawlAcl: "true"
        maxFileSizeInMegaBytes: "50"
        fieldForUserId: user_id
        paymentModel: A
        inclusionTeamNameFilter:
          - TeamA
          - TeamB
        exclusionTeamNameFilter:
          - TeamC
        inclusionChannelNameFilter:
          - Channel1
          - Channel2
        exclusionChannelNameFilter:
          - Channel3
        inclusionFileNamePatterns:
          - "*.docx"
          - "*.pdf"
        exclusionFileNamePatterns:
          - "*.tmp"
        inclusionFileTypePatterns:
          - image/png
          - image/jpeg
        exclusionFileTypePatterns:
          - application/octet-stream
        inclusionUserEmailFilter:
          - user@example.com
        isCrawlChatMessage: "true"
        isCrawlChatAttachment: "true"
        isCrawlChannelPost: "true"
        isCrawlChannelAttachment: "true"
        isCrawlChannelWiki: "true"
        isCrawlCalendarMeeting: "true"
        isCrawlMeetingChat: "true"
        isCrawlMeetingFile: "true"
        isCrawlMeetingNote: "true"
        startCalendarDateTime: "2023-01-01T00:00:00Z"
        endCalendarDateTime: "2023-12-31T23:59:59Z"
        enableDeletionProtection: "false"
```

```
        deletionProtectionThreshold: "15"
```

> **Note**
>
> ACL crawling is available for both new and original Microsoft Teams connector versions.

How Amazon Q Business connector crawls Microsoft Teams ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

Microsoft Teams content is categorized into Chats, Channels, and Calendar. Chats support one-on-one and group conversations with attachments, which can be filtered using email domains or regex rules. Channels are structured within Microsoft Teams and can be Standard (open to all team members), Shared (accessible to team members and invited external users), or Private (restricted to specific members). Calendars facilitate meeting scheduling and management, supporting attachments and OneNote tabs.

When you connect a Microsoft Teams data source to Amazon Q Business, Amazon Q Business makes a copy of these resources and creates an index that can be used to respond to user prompts and queries. Additionally, the connector crawls ACL information attached to a document (user and group information) from your Microsoft Teams instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

Identity Crawling: Amazon Q Business synchronizes both local and federated users/groups. Federated groups are synced outside Amazon Q, and their memberships are not stored. Identities are canonicalized by converting all letters to lowercase to prevent duplication issues, meaning "TestUser" and "testuser" are treated as the same. When a user is deleted, their permissions are not inherited by a newly created user with the same name, ensuring secure access management. Once a user is marked as disabled in Microsoft Teams, after the next sync users will no longer have access to search or retrieve previously crawled data, including calendar meetings.

Users can configure the connector to include filters for channel posts and attachments. Team and Channel name can be included and excluded. Also, we can add regular expression to include

and exclude filters for attachments. Private channels are restricted to specific members within a team. Shared and private channels have their own ACLs, enabling more granular permission management.

Permission Inheritance: Chats, Channels and Calendar inherit permissions from the root or the group while attachments inherit from their parent entity (chat, channel, or calendar event).

Change Management: Change Log Mode in Amazon Q Business enables incremental updates by capturing modifications made to content in Microsoft Teams. Instead of re-indexing all documents, it indexes only newly added, updated, or deleted items since the last crawl. Any changes to user or group access permissions are also recorded, ensuring accurate and up-to-date indexing.

Failure handling: The connector follows a fail-close approach, meaning if there are permission-related issues or API failures, affected documents are skipped from ingestion rather than being made publicly accessible. This prevents unauthorized access while maintaining data integrity.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

> **Note**
>
> Field mappings are available for the original Microsoft Teams connector only. The new connector uses automatic field mapping.

Microsoft Teams data source connector field mappings

To help you structure data for retrieval and chat filtering, Amazon Q Business crawls data source document attributes or metadata and maps them to fields in your Amazon Q index.

Amazon Q has reserved fields that it uses when querying your application. When possible, Amazon Q automatically maps these built-in fields to attributes in your data source. If a built-in field doesn't have a default mapping, or if you want to map additional index fields, use the custom field mappings to specify how a data source attribute maps to your Amazon Q application. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

Important

Filtering using document attributes in chat is only supported through the API.

The Amazon Q Teams connector supports the following entities and the associated reserved and custom attributes.

Note

You can map any Teams field to the document title or document body Amazon Q reserved/default index fields.

Supported entities and field mappings

- Chat messages
- Chat attachments
- Channel posts
- Channel file attachments
- Wiki
- Meeting chats
- Meeting details
- Meeting notes
- Meeting files

Chat messages

Microsoft Teams field name	Index field name	Description	Data type
subject	tms_subject	Custom	String
summary	tms_summary	Custom	String

Microsoft Teams field name	Index field name	Description	Data type
importance	tms_importance	Custom	String
messageType	tms_message_type	Custom	String
sender	tms_sender	Custom	String
sourceUrl	_source_uri	Default	String
attachments	tms_attachments	Custom	String list
reactions	tms_reactions	Custom	String list
mentions	tms_mentions	Custom	String list
deletedAt	tms_last_deleted_at	Custom	Date
createdAt	_created_at	Default	Date
lastModifiedAt	_last_updated_at	Default	Date

Chat attachments

Microsoft Teams field name	Index field name	Description	Data type
fileName	tms_name	Custom	String
size	tms_file_size	Custom	Long (numeric)
title	tms_title	Custom	String
sourceUrl	_source_uri	Default	String
lastModifiedBy	tms_last_modified_by	Custom	String
createdBy	tms_created_by	Custom	String

Microsoft Teams field name	Index field name	Description	Data type
createdAt	_created_at	Default	Date
lastModifiedAt	_last_updated_at	Default	Date

Channel posts

Microsoft Teams field name	Index field name	Description	Data type
subject	tms_subject	Custom	String
summary	tms_summary	Custom	String
importance	tms_importance	Custom	String
messageType	tms_message_type	Custom	String
createdBy	tms_created_by	Custom	String
deletedAt	tms_last_deleted_at	Custom	Date
sourceUrl	_source_uri	Default	String
mentions	tms_mentions	Custom	String list
reactions	tms_reactions	Custom	String list
attachments	tms_attachments	Custom	String list
createdAt	_created_at	Default	Date
lastModifiedAt	_last_updated_at	Default	Date

Channel file attachments

Microsoft Teams field name	Index field name	Description	Data type
fileName	tms_name	Custom	String
size	tms_file_size	Custom	Long (numeric)
channelName	tms_channel_name	Custom	String
Title	tms_title	Custom	String
sourceUrl	_source_uri	Default	String
createdBy	tms_created_by	Custom	String
lastModifiedBy	tms_last_modified_by	Custom	String
createdAt	_created_at	Default	Date
lastModifiedAt	_last_updated_at	Default	Date
oneNoteDocument	tms_onenote_document	Custom	String
oneNoteSection	tms_onenote_section	Custom	String
oneNotePage	tms_onenote_page	Custom	String

Wiki

Microsoft Teams field name	Index field name	Description	Data type
channelName	tms_channel_name	Custom	String
fileName	tms_name	Custom	String

Microsoft Teams field name	Index field name	Description	Data type
size	tms_file_size	Custom	Long (numeric)
createdBy	tms_created_by	Custom	String
lastModifiedBy	tms_last_modified_by	Custom	String
title	tms_title	Custom	String
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
lastModifiedAt	_last_updated_at	Default	Date

Meeting chats

Microsoft Teams field name	Index field name	Description	Data type
subject	tms_subject	Custom	String
summary	tms_summary	Custom	String
importance	tms_importance	Custom	String
messageType	tms_message_type	Custom	String
Sender	tms_sender	Custom	String
attachments	tms_attachments	Custom	String list
mentions	tms_mentions	Custom	String list
reactions	tms_reactions	Custom	String list
sourceUrl	_source_uri	Default	String

Microsoft Teams field name	Index field name	Description	Data type
deletedAt	tms_last_deleted_at	Custom	Date
createdAt	_created_at	Default	Date
lastModifiedAt	_last_updated_at	Default	Date

Meeting details

Microsoft Teams field name	Index field name	Description	Data type
subject	tms_subject	Custom	String
summary	tms_summary	Custom	String
importance	tms_importance	Custom	String
username	tms_from_user	Custom	String
eventStartTime	tms_event_start_time	Custom	Date
eventEndTime	tms_event_end_time	Custom	Date
sourceURL	_source_uri	Default	String

Meeting notes

Microsoft Teams field name	Index field name	Description	Data type
fileName	tms_name	Custom	String
title	tms_title	Custom	String
createdBy	tms_created_by	Custom	String

Microsoft Teams field name	Index field name	Description	Data type
lastModifiedBy	tms_last_modified_by	Custom	String
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
lastModifiedAt	_last_updated_at	Default	Date

Meeting files

Microsoft Teams field name	Index field name	Description	Data type
fileName	tms_name	Custom	String
title	tms_title	Custom	String
size	tms_file_size	Custom	Long (numeric)
sourceUrl	_source_uri	Default	String
createdBy	tms_created_by	Custom	String
lastModifiedBy	tms_last_modified_by	Custom	String
createdAt	_created_at	Default	Date
lastModifiedAt	_last_updated_at	Default	Date

IAM role for Microsoft Teams connector

> **Note**
>
> This section applies to both new and original Microsoft Teams connector versions.

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
```

```
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
```

```
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
```

```
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Troubleshooting your Microsoft Teams connector

The following table provides information about error codes you might see for the Microsoft Teams connector and suggested troubleshooting actions.

Error code	Error message	Suggested resolution
MST-5001	Exception occurred while sending request to MSTeams api, please try again later.	Error related to authentication. Check logs for the specific error message.
MST-5101	Exception occurred while validating configuration.	Error related to configurations. Check logs for the specific error message.
MST-5102	ClientID cannot be null in Repository configuration.	Error related to configurations. Check logs for the specific error message.

Error code	Error message	Suggested resolution
MST-5103	TenantId cannot be null in Repository configura tion.	Error related to configurations. Check logs for the specific error message.
MST-5104	ClientSecret cannot be null in Repository configuration	Error related to configurations. Check logs for the specific error message.
MST-5105	Please add a valid paymentModel under additionalProperties. The paymentModel should be one of the following.	Error related to configurations. Check logs for the specific error message.
MST-5106	Please add valid startCalendarDateTime & endCalendarDateTime under additionalProperti es: startCalendarDateT ime & endCalend arDateTime should be in this format 2016-12-0 1T00:00:00Z.	Error related to configurations. Please check logs for the specific error message.
MST-5107	isCrawlChatMessage should be true or false.	Error related to configurations. Please check logs for the specific error message.
MST-5108	isCrawlMeetingChatValue should be true or false.	Error related to configurations. Please check logs for the specific error message.
MST-5109	isCrawlChatAttachment should be true or false.	Error related to configurations. Please check logs for the specific error message.

Error code	Error message	Suggested resolution
MST-5110	isCrawlMeetingFile should be true or false.	Error related to configurations. Please check logs for the specific error message.
MST-5111	isCrawlMeetingNote should be true or false.	Error related to configurations. Please check logs for the specific error message.
MST-5112	isCrawlChannelPost should be true or false.	Error related to configurations. Please check logs for the specific error message.
MST-5113	isCrawlChannelAttachment should be true or false	Error related to configurations. Please check logs for the specific error message.
MST-5114	isCrawlChannelWiki should be true or false.	Error related to configurations. Please check logs for the specific error message.
MST-5115	isCrawlCalendarMeeting should be true or false.	Error related to configurations. Please check logs for the specific error message.
MST-5116	Invalid clientId pattern.	Error related to configurations. Please check logs for the specific error message..
MST-5117	ClientSecret Over maximum length.	Error related to configurations. Please check logs for the specific error message.
MST-5200	Got exception from customer while accessing list of users.	Failure while fetching the list of users from Microsoft Graph API. Please check logs for more details.

Error code	Error message	Suggested resolution
MST-5201	Got exception from customer while accessing list of chats.	Failure while fetching the list of chats from Microsoft Graph API. Please check logs for more details.
MST-5202	Got exception from customer while accessing meeting chats.	Failure while fetching meeting chats from Microsoft Graph API. Please check logs for more details.
MST-5203	Got exception from customer while accessing list of groups.	Failure while fetching the list of groups from Microsoft Graph API. Please check logs for more details.
MST-5204	Got exception from customer while accessing list of channels.	Failure while fetching the list of channels from Microsoft Graph API. Please check logs for more details.
MST-5205	Error occurred while fetching meeting events.	Failure while fetching meeting events from Microsoft Graph API. Please check logs for more details.
MST-5206	Error occurred while fetching drive files.	Failure while fetching drive files from Microsoft Graph API. Please check logs for more details.
MST-5207	Error while Interrupt edException rate limit.	Failures while retrying API requests to fetch data from Microsoft Graph API.
MST-5209	Got exception from customer while running full crawl.	Failures while running full crawl iterator. Please refer logs or contact connector team for more information.
MST-5210	Exception occurred while accessing list of channel attachment from data source.	Failure while fetching the list of channels attachment from Microsoft Graph API. Please check logs for more details.

Error code	Error message	Suggested resolution
MST-5211	Exception occurred while accessing meeting chat information for user.	Failure while accessing meeting chats from Microsoft Graph API. Please check logs for more details.
MST-5212	Exception occurred while processing to access list of users.	Failure while processing to access list of users from Microsoft Graph API. Please check logs for more details.
MST-5213	Exception occurred while processing to access list of groups.	Failure while processing to access list of groups from Microsoft Graph API. Please check logs for more details.
MST-5214	Exception occurred while processing to access list of channel attachment.	Failure while processing to access list of channel attachment from Microsoft Graph API. Please check logs for more details.
MST-5215	Exception occurred while processing to access meeting events.	Failure while processing to access meeting events from Microsoft Graph API. Please check logs for more details.
MST-5301	Got exception from customer while running changelog.	Failures while handling changelog token. Please refer logs or contact connector team for more information.
MST-5302	Error in serializing change log token.	Failures while serializing change log token. Please refer logs or contact connector team for more information.
MST-5303	Error in de-serializing change log token.	Failures while de-serializing change log token. Please refer logs or contact connector team for more information.
MST-5400	Exception occurred while running Identity Crawler.	Error occurred while fetching groups details from Microsoft Graph API. Please check logs for more details.

Error code	Error message	Suggested resolution
MST-5401	Error while build groups details for Identity Crawler.	Failures while de-serializing change log token. Please refer logs or contact connector team for more information.
MST-5500	Exception occurred while getting file content response.	Error occurred while fetching file content response details from Microsoft Graph API. Please check logs for more details.
MST-5501	Only String, String List, Date and Long formats are supported for field mappings.	Error related to unsupported field mappings. Please check logs for the specific error message.
MST-5502	IO Exception occurred.	IO Exception.

Connecting Amazon S3 to Amazon Q Business

Amazon Simple Storage Service (Amazon S3) is an object storage service that stores data as objects within storage buckets. You can connect an Amazon S3 instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

After you integrate Amazon Q with Amazon S3, users can ask questions about the content stored in Amazon S3. For example, a user might ask about the main points discussed in a blog post on cloud security, the installation steps outlined in a user guide, findings from a case study on hybrid cloud usage, market trends noted in an analyst report, or key takeaways from a whitepaper on data encryption. This integration helps users to quickly find the specific information they need, improving their understanding and ability to make informed business decisions.

Amazon Q Business supports source attribution with citations. If you specify the `_source_uri` metadata field when you add metadata to your Amazon S3 bucket, the source attribution links returned by Amazon Q Business in the chat results will direct users to the configured URL. If you don't specify a `_source_uri`, users can still access the source documents through clickable citation links that will download the file at query time. This allows users to verify information even

when no source URI is configured. To learn how to add metadata for your Amazon S3 connector, see Adding document metadata in Amazon S3.

> **Note**
>
> To learn how to create an Amazon S3 bucket, see Creating a bucket in the *Amazon Simple Storage Service User Guide*.

Topics

- Connecting Amazon S3 to Amazon Q Business using the New connector
- Connecting Amazon S3 to Amazon Q Business (Old)

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Connecting Amazon S3 to Amazon Q Business using the New connector

> **Note**
>
> **Enhanced Version:** With the new connector, you can refresh your index significantly faster than before.

Known limitations

The Amazon S3 connector has the following known limitations:

- The Amazon S3 bucket must be in the same AWS Region as your Amazon Q index, and your index must have permissions to access the bucket that contains your documents.

- VPC connectivity not supported (use the old version if VPC support is required)
- Custom field mappings not supported (use the old connector version if required)
- Document enrichment is not supported. (use the old connector version if required)

Overview

The following table gives an overview of the Amazon Q Business Amazon S3 connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Assume Role Based
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	No. Use User Store APIs if you want to crawl users and groups.
Crawl features	**Custom metadata**	No
	Entities	Yes. The following entities are supported: • Document See What is a document? for more details on what each connector crawls as a document.
	Filters	Yes. The following filters are supported: • Include/exclude by prefix (for example `Data/`, where `Data` is a folder containing documents) • Include/exclude by file types (for example `.*\.pdf`, or `.*\.txt`)

Category	Feature	Support
		• Include/exclude by glob patterns (for example `*.java`, which specifies a pattern that represents file names ending in `.java`)
	File types	Supports all files supported by Amazon Q.

Prerequisites

Before you begin, make sure that you have completed the following prerequisites.

In Amazon S3, make sure you have:

- Created an Amazon S3 bucket and copied it's name.

> **Note**
>
> Your bucket must be in the same AWS Region as your Amazon Q index, and your index must have permissions to access the bucket that contains your documents.

Using the console

The following procedure outlines how to connect Amazon Q Business to Amazon S3 using the AWS Management Console.

Connecting Amazon Q to Amazon S3

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Amazon S3** data source to your Amazon Q application.
5. Then, on the **Amazon S3** data source page, enter the following information:
6. **Name and description**, do the following:

    - For **Data source name** – Name your data source for easy tracking.

> **Note**
>
> You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> IAM roles used for applications can't be used for data sources. If you are unsure if an existing role is used for an application, choose **Create a new role** to avoid errors.

8. **Data source location** – Choose the location of your Amazon S3 bucket:

   a. **This account** – Selected by default. Choose this option if your Amazon S3 bucket is in the same account as your Amazon Q Business application.

   b. **Other account** – Choose this option if your Amazon S3 bucket is in a different account.

      - **Account ID** – Specify the ID for the other account that owns the bucket.

9. **Sync scope**, enter the following information:

   a. **Enter the data source location** – The path to the Amazon S3 bucket where your data is stored.

      - If you selected **This account**, you can select **Browse S3** to find and choose your bucket.
      - If you selected **Other account**, you must manually enter the bucket name as the browse option is not available for cross-account buckets.

> **Note**
>
> Your bucket must be in the same AWS Region as your Amazon Q Business index.

b. **Maximum file size - *optional*** – You can specify the file size limit in MB for Amazon Q crawling. Amazon Q crawls only files within the defined size limit. The default file size is 50MB. The maximum file size limit is 10 GB.

c. **Access control list configuration file location - *optional*** – The path to the location of a file containing a JSON structure that specifies access settings for the files stored in your S3 data source.

- If you selected **This account**, you can select **Browse S3** to locate your ACL file.
- If you selected **Other account**, you must manually enter the file path as the browse option is not available for cross-account buckets.

d. **Metadata files folder location - *optional*** – The path to the folder in which your metadata is stored.

- If you selected **This account**, you can select **Browse S3** to locate your metadata folder.
- If you selected **Other account**, you must manually enter the folder path as the browse option is not available for cross-account buckets.

e. **Filter patterns** – Add regex patterns to include or exclude documents from your index.

To include or exclude files and folders, you can use a prefix filter (for example `Data/`, where `Data` is a folder containing documents in your S3 bucket). You can also filter using glob patterns and file types.

f. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**. For more information, see Extracting semantic meaning from embedded images and visuals.

To extract audio transcriptions and video content, enable **Audio Files**. To extract video content, enable **Video files**. For more information, see Extracting semantic meaning from audio and video Content.

g. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

10. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
11. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
12. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Amazon S3 using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- Amazon S3 configuration properties
- Amazon S3 JSON schema
- Amazon S3 JSON schema example

Amazon S3 configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`type`	The type of data source. Specify `S3V2` as your data source type.	`string` The only allowed value is `S3V2`.	Yes
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has sub-properties: `bucketName` and `bucketOwnerAccountId` .	Yes
`bucketName`	The name of your Amazon S3 bucket. This is a sub-property for the `connectionConfiguration` .	`string`	Yes
`bucketOwnerAccountId`	The 12-digit AWS account ID that owns the S3 bucket. This is a sub-property for the `connectionConfiguration` .	`string` Must match pattern: `^\d{12}$`	Yes
`filterConfiguration`	Configuration for filtering which files to include or exclude from indexing.	`object` This property has sub-properties for patterns, prefixes, and file size limits.	No

Configuration	Description	Type	Required
`inclusionPatterns`	File patterns to include during indexing . This is a sub-property for the `filterConfiguration` .	`array` of `string`	No
`exclusionPatterns`	File patterns to exclude during indexing. This is a sub-property for the `filterConfiguration` .	`array` of `string`	No
`inclusionPrefixes`	S3 key prefixes to include during indexing (e.g., documents/, reports/). This is a sub-property for the `filterConfiguration` .	`array` of `string`	No
`exclusionPrefixes`	S3 key prefixes to exclude during indexing (e.g., temp/, cache/). This is a sub-property for the `filterConfiguration` .	`array` of `string`	No

Configuration	Description	Type	Required
`maxFileSizeInMegaBytes`	Maximum file size in megabytes to index. Files larger than this will be skipped. This is a sub-property for the `filterConfiguration` .	`number` Minimum: 0, Maximum: 10240	No
`accessControlConfiguration`	Configuration for access control and permissions.	`object` This property has sub-properties for ACL configuration and default access type.	No
`aclConfigurationFilePath`	Path to the ACL configuration file in your S3 bucket. This is a sub-property for the `accessControlConfiguration` .	`string` Length: 1-1024 characters	No
`deletionProtectionConfiguration`	Configuration for deletion protection to prevent accidental bulk deletions.	`object` This property has sub-properties for enabling deletion protection and setting thresholds.	No

Configuration	Description	Type	Required
`enableDeletionProtection`	Whether to enable deletion protection. This is a sub-property for the `deletionProtectionConfiguration` .	`boolean`	No
`deletionProtectionThreshold`	Percentage threshold for deletion protection. If more than this percentage of documents would be deleted, the sync will be blocked. This is a sub-property for the `deletionProtectionConfiguration` .	`number` Default: 15	No
`metadataFilesPrefix`	S3 key prefix where metadata files are stored for enhanced document processing.	`string` Length: 1-1024 characters	No

Amazon S3 JSON schema

The following is the Amazon S3 JSON schema with simplified configuration structure:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "pattern": "S3V2"
    },
    "connectionConfiguration": {
```

```
      "type": "object",
      "properties": {
        "bucketName": {
          "type": "string"
        },
        "bucketOwnerAccountId": {
          "type": "string",
          "pattern": "^\\d{12}$"
        }
      },
      "required": ["bucketName", "bucketOwnerAccountId"]
    },
    "filterConfiguration": {
      "type": "object",
      "properties": {
        "inclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionPrefixes": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionPrefixes": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "maxFileSizeInMegaBytes": {
          "type": "number",
          "minimum": 0,
          "maximum": 10240
        }
```

```
      }
    },
    "accessControlConfiguration": {
      "type": "object",
      "properties": {
        "aclConfigurationFilePath": {
          "type": "string",
          "minLength": 1,
          "maxLength": 1024
        }
      }
    },
    "deletionProtectionConfiguration": {
      "type": "object",
      "properties": {
        "enableDeletionProtection": {
          "type": "boolean"
        },
        "deletionProtectionThreshold": {
          "type": "number",
          "default": 15
        }
      }
    },
    "metadataFilesPrefix": {
      "type": "string",
      "minLength": 1,
      "maxLength": 1024
    }
  },
  "required": [
    "type",
    "connectionConfiguration"
  ]
}
```

Amazon S3 JSON schema example

The following is the Amazon S3 JSON schema example with simplified configuration:

```
{
  "type": "S3V2",
  "connectionConfiguration": {
    "bucketName": "my-company-data-bucket",
```

```
    "bucketOwnerAccountId": "123456789012"
  },
  "filterConfiguration": {
    "inclusionPrefixes": ["documents/", "reports/"],
    "exclusionPrefixes": ["temp/", "cache/"],
    "maxFileSizeInMegaBytes": 100
  },
  "accessControlConfiguration": {
    "aclConfigurationFilePath": "config/acl-config.json"
  },
  "deletionProtectionConfiguration": {
    "enableDeletionProtection": true,
    "deletionProtectionThreshold": 15
  },
  "metadataFilesPrefix": "metadata/"
}
```

Connecting Amazon Q Business to Amazon S3 using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- Amazon S3 configuration properties
- Amazon S3 JSON schema for using the configuration property with AWS CloudFormation
- Amazon S3 YAML schema for using the configuration property with AWS CloudFormation

Amazon S3 configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
type	The type of data source. Specify S3V2 as your data source type.	string The only allowed value is S3V2.	Yes
connectionConfiguration	Configuration information for the endpoint for the data source.	object This property has sub-properties: bucketName and bucketOwnerAccountId .	Yes
bucketName	The name of your Amazon S3 bucket. This is a sub-property for the connectionConfiguration .	string	Yes
bucketOwnerAccountId	The 12-digit AWS account ID that owns the S3 bucket. This is a sub-property for the connectionConfiguration .	string Must match pattern: ^\d{12}$	Yes
filterConfiguration	Configuration for filtering which files to include or exclude from indexing.	object This property has sub-properties for patterns, prefixes, and file size limits.	No
inclusionPatterns	File patterns to include during indexing . This is a	array of string	No

Configuration	Description	Type	Required
	sub-property for the `filterConfiguration`.		
`exclusionPatterns`	File patterns to exclude during indexing. This is a sub-property for the `filterConfiguration`.	`array` of `string`	No
`inclusionPrefixes`	S3 key prefixes to include during indexing (e.g., documents/, reports/). This is a sub-property for the `filterConfiguration`.	`array` of `string`	No
`exclusionPrefixes`	S3 key prefixes to exclude during indexing (e.g., temp/, cache/). This is a sub-property for the `filterConfiguration`.	`array` of `string`	No
`maxFileSizeInMegaBytes`	Maximum file size in megabytes to index. Files larger than this will be skipped. This is a sub-property for the `filterConfiguration`.	`number` Minimum: 0, Maximum: 10240	No

Configuration	Description	Type	Required
`accessControlConfiguration`	Configuration for access control and permissions.	`object` This property has sub-properties for ACL configuration and default access type.	No
`aclConfigurationFilePath`	Path to the ACL configuration file in your S3 bucket. This is a sub-property for the `accessControlConfiguration` .	`string` Length: 1-1024 characters	No
`deletionProtectionConfiguration`	Configuration for deletion protection to prevent accidental bulk deletions.	`object` This property has sub-properties for enabling deletion protection and setting thresholds.	No
`enableDeletionProtection`	Whether to enable deletion protection. This is a sub-property for the `deletionProtectionConfiguration` .	`boolean`	No

Configuration	Description	Type	Required
`deletionProtectionThreshold`	Percentage threshold for deletion protection. If more than this percentage of documents would be deleted, the sync will be blocked. This is a sub-property for the `deletionProtectionConfiguration` .	`number` Default: 15	No
`metadataFilesPrefix`	S3 key prefix where metadata files are stored for enhanced document processing.	`string` Length: 1-1024 characters	No

Amazon S3 JSON schema for using the configuration property with AWS CloudFormation

The following is the Amazon S3 JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- Amazon S3 JSON schema for using the configuration property with AWS CloudFormation
- Amazon S3 JSON schema example for using the configuration property with AWS CloudFormation

Amazon S3 JSON schema for using the configuration property with AWS CloudFormation

The following is the Amazon S3 JSON schema for the configuration property for CloudFormation.

```
{
  "type": "object",
  "properties": {
    "type": {
```

```
      "type": "string",
      "pattern": "S3V2"
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "bucketName": {
          "type": "string"
        },
        "bucketOwnerAccountId": {
          "type": "string",
          "pattern": "^\\d{12}$"
        }
      },
      "required": ["bucketName", "bucketOwnerAccountId"]
    },
    "filterConfiguration": {
      "type": "object",
      "properties": {
        "inclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionPrefixes": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionPrefixes": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "maxFileSizeInMegaBytes": {
```

```
          "type": "number",
          "minimum": 0,
          "maximum": 10240
        }
      }
    },
    "accessControlConfiguration": {
      "type": "object",
      "properties": {
        "aclConfigurationFilePath": {
          "type": "string",
          "minLength": 1,
          "maxLength": 1024
        }
      }
    },
    "deletionProtectionConfiguration": {
      "type": "object",
      "properties": {
        "enableDeletionProtection": {
          "type": "boolean"
        },
        "deletionProtectionThreshold": {
          "type": "number",
          "default": 15
        }
      }
    },
    "metadataFilesPrefix": {
      "type": "string",
      "minLength": 1,
      "maxLength": 1024
    }
  },
  "required": [
    "type",
    "connectionConfiguration"
  ]
}
```

Amazon S3 JSON schema example for using the configuration property with AWS CloudFormation

The following is the Amazon S3 JSON example for the Configuration property for CloudFormation.

```
{
  "type": "S3V2",
  "connectionConfiguration": {
    "bucketName": "my-company-data-bucket",
    "bucketOwnerAccountId": "123456789012"
  },
  "filterConfiguration": {
    "inclusionPatterns": ["*.pdf", "*.docx", "*.txt"],
    "exclusionPatterns": ["*.tmp", "*.log"],
    "inclusionPrefixes": ["documents/", "reports/"],
    "exclusionPrefixes": ["temp/", "cache/"],
    "maxFileSizeInMegaBytes": 100
  },
  "accessControlConfiguration": {
    "aclConfigurationFilePath": "config/acl-config.json"
  },
  "deletionProtectionConfiguration": {
    "enableDeletionProtection": true,
    "deletionProtectionThreshold": 15
  },
  "metadataFilesPrefix": "metadata/"
}
```

Amazon S3 YAML schema for using the configuration property with AWS CloudFormation

The following is the Amazon S3 YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- Amazon S3 YAML schema example for using the configuration property with AWS CloudFormation

Amazon S3 YAML schema example for using the configuration property with AWS CloudFormation

The following is the Amazon S3 YAML example for the Configuration property for CloudFormation:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: "CloudFormation Amazon S3 Data Source Template"
Resources:
  DataSourceS3V2:
    Type: "AWS::QBusiness::DataSource"
    Properties:
      ApplicationId: app12345-1234-1234-1234-123456789012
      IndexId: indx1234-1234-1234-1234-123456789012
      DisplayName: MyS3DataSourceV2
      RoleArn: arn:aws:iam::123456789012:role/qbusiness-data-source-role
      Configuration:
        type: S3V2
        connectionConfiguration:
          bucketName: my-company-data-bucket
          bucketOwnerAccountId: "123456789012"
        filterConfiguration:
          inclusionPatterns:
            - "*.pdf"
            - "*.docx"
            - "*.txt"
          exclusionPatterns:
            - "*.tmp"
            - "*.log"
          inclusionPrefixes:
            - "documents/"
            - "reports/"
          exclusionPrefixes:
            - "temp/"
            - "cache/"
          maxFileSizeInMegaBytes: 100
        accessControlConfiguration:
          aclConfigurationFilePath: "config/acl-config.json"
        deletionProtectionConfiguration:
          enableDeletionProtection: true
          deletionProtectionThreshold: 15
        metadataFilesPrefix: "metadata/"
```

IAM role

Whether you use the AWS Management Console or the CreateDataSource API, you must provide an IAM role that allows Amazon Q Business to access your Amazon S3 bucket.

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q Business resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role while creating your data source.

> **Note**
>
> To learn how to create an IAM role, see Create a role to delegate permissions to an AWS service.

Cross-account Amazon S3 buckets are supported with Amazon Q Business. However, your bucket must be located in the same AWS Region as your Amazon Q Business index, and your index must have permissions to access the bucket containing your documents.

When you use an Amazon S3 bucket as a data source, you must provide a role that has permissions to:

- Access your Amazon S3 bucket.
- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` API operations in order to ingest documents.
- Permission to access the Principal Store APIs needed to ingest access control and identity information from documents.

To allow Amazon Q to use an Amazon S3 bucket as a data source, use the following role policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetObjectfromS3",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::{{input_bucket_name}}/*"
      ],
```

```
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "{{account_id}}"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToListS3Buckets",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::{{input_bucket_name}}"
      ],
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "{{account_id}}"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
    },
    {
      "Sid": "AllowsAmazonQToCallPrincipalMappingAPIs",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
```

```
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToPassCustomerRole",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::{{account_id}}:role/QBusiness-DataSource-*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "qbusiness.amazonaws.com"
        }
      }
    }
  ]
}
```

If the documents in the Amazon S3 bucket are encrypted, you must provide the following permissions to use the AWS KMS key to decrypt the documents:

```
{
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
```

```
    }
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

Clickable URLs

The Clickable URL feature allows end users to access source documents through citation links in chat responses, regardless of whether a source URI is configured.

This feature improves the verification experience by making all documents of supported datasource types accessible. Currently, clickable links are only supported for Amazon S3, custom connectors, file upload and direct `BatchPutDocument` ingestion of documents.

Configuration Requirements: While this feature works automatically for new applications, existing customers may need additional configuration:

- If you already use Amazon S3 data source for your Amazon Q Business application, you will need to perform a full sync of the data source for the clickable URLs feature to be available to your users.

- If you already use an Amazon Q Business web experience, you may need to add additional permissions to the IAM role for the web experience. See the troubleshooting section below for details.

Download Concurrency Limit: For information about file size limits, see Quotas and regions.

Access Control: The Clickable URL respects all access control settings:

- If a user's access to a file is revoked after they've viewed it in a chat, once a resync is performed subsequent attempts to access the file will be denied with a clear error message.
- If a file is updated after a chat reference, then once a resync is performed clicking the link will retrieve the current version of the file.
- If a file is deleted and a resync is performed users will receive a clear error message indicating the file no longer exists.

Troubleshooting clickable links

This section helps you resolve errors that you might encounter when using clickable links for source references in your conversations with your Amazon Q Business AI assistant.

Full sync required

> **Note**
>
> The following suggested troubleshooting steps apply only to existing accounts using the Amazon S3 connector.

Issue: When you try to access referenced URLs from an Amazon S3 or uploaded files data source, you receive the following error message.

Error message:

```
This document cannot be downloaded because the raw document download feature requires a
 full connector sync performed after 07/02/2025. Your admin has not yet completed this
 full sync. Please contact your admin to request a complete sync of the data source.
```

Solution: This error occurs when the data source hasn't completed a full sync after the clickable links feature was enabled. To resolve this issue:

- For S3 data sources: Perform a full sync of the S3 data source.
- For uploaded files data sources: Delete the files from the upload files data source and upload them again.

Permission changes

Issue: When browsing conversation history, you click on a reference URL from an Amazon S3 data source but can't view or download the file.

Error message:

```
You no longer have permission to access this document. The access permissions for this
 document have been changed since you last accessed it. Please contact your admin if
 you believe you should have access to this content.
```

Solution: This error occurs when the permissions for the document in the ACLs on the Amazon S3 bucket changed after your conversation, removing your access to the file. The ACLs were updated in the Amazon Q Business index during a subsequent data source sync. If you believe you should have access to the document, contact your administrator to:

- Review and update the ACLs
- Perform a data source sync

Document not found

Issue: When browsing conversation history, you click on a reference URL from an Amazon S3 or upload files data source but can't view or download the file.

Error message:

```
The document you're trying to access no longer exists in the data source. It may have
 been deleted or moved since it was last referenced. Please check with the admin if you
 need access to this document.
```

Solution: This error occurs when the document was deleted from the Amazon S3 bucket, moved to a different location, or deleted from the upload files data source after your conversation. The document was also removed from the Amazon Q Business index and staging bucket during a

subsequent data source sync. If you believe the document shouldn't have been deleted, contact your administrator to restore the document and perform a data source sync.

Insufficient permissions

> **Note**
>
> The following suggested troubleshooting steps apply only to existing accounts using the Amazon S3 connector.

Issue: When you click on a reference URL from an Amazon S3 or upload files data source, you can't view or download the file.

Error message:

```
Unable to download this document because your Web Experience lacks the required
 permissions. Your admin needs to update the IAM role for the Web Experience to include
 permissions for the GetDocumentContent API. Please contact your admin to request this
 IAM role update.
```

Solution: This error occurs when the web experience doesn't have the required permissions to invoke the GetDocumentContent API. Your administrator can resolve this error by updating the IAM role for the web experience with the permissions described in the *Considerations for using S3 clickable URLs* section.

If you already use a Amazon Q Business web experience, add the following permissions to the IAM role for the Amazon Q Business web experience:

```
{
    "Sid": "QBusinessGetDocumentContentPermission",
    "Effect": "Allow",
    "Action": ["qbusiness:GetDocumentContent"],
    "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/*"
    ]
}
```

Adding document metadata in Amazon S3

To customize chat results for your end users, you can add metadata or document attributes to documents in an Amazon S3 bucket by using a metadata file. Metadata is additional information about a document, such as its title and the date and time it was created. To learn more about metadata in Amazon Q Business, see Document attributes in Amazon Q Business.

Amazon Q Business supports source attribution with citations. If you specify the `_source_uri` metadata field when you add metadata to your Amazon S3 bucket, the source attribution links returned by Amazon Q Business in the chat results will direct users to the configured URL. If you don't specify a `_source_uri`, users can still access the source documents through clickable citation links that will download the file at query time. This allows users to verify information even when no source URI is configured.

Topics

- Document metadata location
- Document metadata structure

Document metadata location

In Amazon S3, each metadata file can be associated with an indexed document. Your metadata files must be stored in the same Amazon S3 bucket as your indexed files. You can specify a location within the Amazon S3 bucket for your metadata files by using the AWS Management Console. Or, you can use the `metadataFilesPrefix` field of the Amazon S3 `configuration` parameter using the JSON schema when you create an Amazon S3 data source using the CreateDataSource API.

If you don't specify an Amazon S3 prefix, your metadata files must be stored in the same location as your indexed documents. If you specify an Amazon S3 prefix for your metadata files, they must be in a directory structure parallel to your indexed documents. Amazon Q looks only in the specified directory for your metadata. If the metadata isn't read, check that the directory location matches the location of your metadata.

The following examples show how the indexed document location maps to the metadata file location. The document's Amazon S3 key is appended to the metadata's Amazon S3 prefix and then suffixed with `.metadata.json` to form the metadata file's Amazon S3 path.

> **Note**
>
> The combined Amazon S3 key, the metadata's Amazon S3 prefix, and the `.metadata.json` suffix must be no more than a total of 1,024 characters. We recommend that your Amazon S3 key is less than 1,000 characters to account for additional characters when combining your key with the prefix and suffix.

```
Bucket name:
     s3://bucketName
Document path:
     documents
Metadata path:
     none
File mapping
     s3://bucketName/documents/file.txt ->
        s3://bucketName/documents/file.txt.metadata.json
```

```
Bucket name:
     s3://bucketName
Document path:
     documents/legal
Metadata path:
     metadata
File mapping
     s3://bucketName/documents/legal/file.txt ->
        s3://bucketName/metadata/documents/legal/file.txt.metadata.json
```

Document metadata structure

You define your document metadata itself in a JSON file. The file must be a UTF-8 text file without a BOM marker. The file name of the JSON file must be <*document*>.<*extension*>.metadata.json. In this example, *document* is the name of the document that the metadata applies to and *extension* is the file extension for the document. The document ID must be unique in <*document*>.<*extension*>.metadata.json.

The content of the JSON file uses the following template:

```
{
    "DocumentId": "document ID",
```

```
    "Attributes": {
        "_authors": ["author of the document"],
        "_category": "document category",
        "_created_at": "ISO 8601 encoded string",
        "_last_updated_at": "ISO 8601 encoded string",
        "_source_uri": "document URI",
        "_version": "file version",
        "_view_count": number of times document has been viewed
    },
    "AccessControlList": [
         {
             "Name": "user name",
             "Type": "GROUP | USER",
             "Access": "ALLOW | DENY"
         }
    ],
    "Title": "document title",
    "ContentType": "PDF | HTML | MS_WORD | PLAIN_TEXT | PPT | RTF | XML | XSLT
 | MS_EXCEL | CSV | JSON | MD"
}
```

If you provide a Metadata path, make sure that directory structure inside the metadata directory exactly matches the directory structure of data file.

For example, if the data file location is at `s3://bucketName/documents/legal/file.txt`,

the metadata file location should be at `s3://bucketName/metadata/documents/legal/file.txt.metadata.json`.

All of the attributes and fields are optional, so it's not necessary to include all attributes. However, you must provide a value for each attribute that you want to include; the value can't be empty.

The `_created_at` and `_last_updated_at` metadata fields are ISO 8601 encoded dates. For example, 2012-03-25T12:30:10+01:00 is the ISO 8601 date-time format for March 25, 2012, at 12:30PM (plus 10 seconds) in the Central European Time time zone.

You can use the `AccessControlList` field to filter the response from a query. This way, only certain users and groups have access to documents.

How Amazon Q Business connector crawls Amazon S3 ACLs

You add access control information to a document in an Amazon S3 data source using a metadata file associated with the document. You specify the file using the console or as

the `aclConfigurationFilePath` parameter when you call the `CreateDataSource` or `UpdateDataSource` API and use the `configuration` parameter.

> **Note**
>
> The ACL file and data should be stored in the same Amazon S3 bucket.

The configuration file contains a JSON structure that identifies an Amazon S3 prefix and lists the access settings for the prefix. The prefix can be a path, or it can be an individual file. If the prefix is a path, the access settings apply to all of the files in that path.

You provide three pieces of information in the file:

- The access that the entity should have. You can use `ALLOW` or `DENY`.
- The type of entity. You can use `USER` or `GROUP`.
- The name of the entity.

> **Important**
>
> The system grants ALL users access to prefixes that do NOT appear in the ACL file.

The JSON structure for the configuration file must be in the following format:

```
[
    {
        "keyPrefix": "s3://BUCKETNAME/prefix1/",
        "aclEntries": [
            {
                "Name": "user1@example.com",
                "Type": "USER",
                "Access": "ALLOW"
            },
            {
                "Name": "group1",
                "Type": "GROUP",
                "Access": "DENY"
            }
```

```
        ]
    },
    {
        "keyPrefix": "s3://BUCKETNAME/prefix2/",
        "aclEntries": [
            {
                "Name": "user2@example.com",
                "Type": "USER",
                "Access": "ALLOW"
            },
            {
                "Name": "user1@example.com",
                "Type": "USER",
                "Access": "DENY"
            },
            {
                "Name": "group1",
                "Type": "GROUP",
                "Access": "DENY"
            }
        ]
    }
]
```

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Connecting Amazon S3 to Amazon Q Business (Old)

> **Note**
>
> For new implementations, we recommend using the new Amazon S3 connector which enables you to refresh your index significantly faster than before. The new Amazon S3 connector doesn't support VPC, document enrichment, and custom metadata. If you need these features, you can continue using the older Amazon S3 connector.

Known limitations for the connector

The Amazon S3 connector has the following known limitations:

- The Amazon S3 bucket must be in the same AWS Region as your Amazon Q index, and your index must have permissions to access the bucket that contains your documents.

Overview

The following table gives an overview of the Amazon Q Business Amazon S3 connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Assume Role Based
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	No. Use User Store APIs if you want to crawl users and groups.
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Document See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported:

Category	Feature	Support
		• Include/exclude by prefix (for example `Data/`, where `Data` is a folder containing documents) • Include/exclude by file types (for example `.*\.pdf`, or `.*\.txt`) • Include/exclude by glob patterns (for example `*.java`, which specifies a pattern that represents file names ending in `.java`)
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites

Before you begin, make sure that you have completed the following prerequisites.

In Amazon S3, make sure you have:

- Created an Amazon S3 bucket and copied it's name.

  > **Note**
  >
  > Your bucket must be in the same AWS Region as your Amazon Q index, and your index must have permissions to access the bucket that contains your documents.

- If using Amazon VPC with Amazon S3 connector, made sure that you have assigned an Amazon S3 endpoint to your virtual private cloud (VPC). For more information about configuring an Amazon S3 connector with Amazon VPC, see Using Amazon VPC with Amazon S3.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.

- Stored your Amazon S3 authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Amazon S3 using the console

The following procedure outlines how to connect Amazon Q Business to Amazon S3 using the AWS Management Console.

Connecting Amazon Q to Amazon S3

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Amazon S3** data source to your Amazon Q application.
5. Then, on the **Amazon S3** data source page, enter the following information:
6. **Name and description**, do the following:
   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> IAM roles used for applications can't be used for data sources. If you are unsure if an existing role is used for an application, choose **Create a new role** to avoid errors.

8. **Sync scope**, enter the following information:

   a. **Enter the data source location** – The path to the Amazon S3 bucket where your data is stored. Select **Browse S3** to find and choose your bucket.

   > **Note**
   >
   > Your bucket must be in the same AWS Region as your Amazon Q Business index.

   b. **Maximum file size - *optional*** – You can specify the file size limit in MB for Amazon Q crawling. Amazon Q crawls only files within the defined size limit. The default file size is 50MB. The maximum file size limit is 10 GB. Files must be larger than 0 MB and no larger than 10 GB. You can go up to 10 GB (10240 MB) if you enable **Video files** in **Multi-media content** configuration, and up to 2 GB (2048 MB) if you enable **Audio files** in **Multi-media content configuration**.

   c. **Access control list configuration file location - *optional*** – The path to the location of a file containing a JSON structure that specifies access settings for the files stored in your S3 data source. Select **Browse S3** to locate your ACL file.

      For more information, see ACL crawling.

   d. **Metadata files folder location - *optional*** – The path to the folder in which your metadata is stored. Select **Browse S3** to locate your metadata folder.

   e. **Filter patterns** – Add regex patterns to include or exclude documents from your index. All paths are relative to the data source location Amazon S3 bucket. You can add up to 100 patterns.

      You can include and exclude documents using file names, file types, file paths, and glob patterns (patterns that can expand a wildcard pattern into a list of path names that match the given pattern).

      Examples of glob patterns include:

- `/myapp/config/*` – All files inside config directory
- `/**/*.png` – All .png files in all directories
- `/**/*.{png,ico,md}` – All .png, .ico, or .md files in all directories
- `/myapp/src/**/*.ts` – All .ts files inside src directory (and all its subdirectories)
- `**/!(*.module).ts` – All .ts files but not `.module.ts`
- For the following examples, assume that the Amazon S3 bucket is structured like this:

```
S3 bucket:
  - file1.txt
  - file2.txt
  - file3.txt
  - certificate
    - certificate0.cer
    - extra
      - certificate-e.cer
      - extra1
        - certificate-e-1.cer
  - folder1
    - file1-1.txt
    - file1-2.txt
    - file1-3.txt
    - certificate
      - certificate1.cer
  - folder2
    - folder2-1
      - file2-1-1.txt
      - file2-1-2.txt
      - file2-1-3.txt
      - certificate
         - certificate2.cer
```

- ** matches any level * – only matches one level
- **/certificate/**– matches certificate folder at any level except root level (ex. folder2/folder2-1/certificate)
- */certificate/**– matches certificate folder only one level under root level. (ex. like folder1/certificate)

- certificate/**– matches certificate folder at root level. (ex. certificate/ , certificate/extra/ , certificate/extra/extra1)
- To exclude everything inside any "certificate" folder, regardless of its location, use the following:

  certificate/** + **/certificate/**
- Note that `/certificate/**` matches nothing

f. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**. For more information, see Extracting semantic meaning from embedded images and visuals.

To extract audio transcriptions and video content, enable **Audio Files**. To extract video content, enable **Video files**. For more information, see Extracting semantic meaning from audio and video Content.

g. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

9. **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

- **Full sync** – Sync all content regardless of the previous sync status.
- **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

10. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
11. **Configure VPC and security group – *optional*** – You can choose to use a VPC if your Amazon S3 bucket is not accessible through the public internet. If you so, you must add **Subnets** and **VPC security groups** as well.

Important

Make sure you have:

- Configured your VPC according to the steps in Gateway endpoints for Amazon S3.
- Chosen a private subnet in an Amazon Q supported availability zone.
- Configured your security group to allow Amazon Q to access the Amazon S3 endpoint.

For more information, see Using Amazon VPC and Using Amazon VPC with Amazon S3.

If you choose to use VPC, enter the following information:

a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

12. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
13. **Field mappings** – A list of data source document attributes to map to your index fields.

Note

Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

14. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Amazon S3 using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- Amazon S3 configuration properties
- Amazon S3 JSON schema

- Amazon S3 JSON schema example

Amazon S3 configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`type`	The type of data source. Specify S3 as your data source type.	`string` The only allowed value is S3 .	Yes
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	`string` You can choose from the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your	Yes

Configuration	Description	Type	Required
		data source syncs with your index	
connectionConfiguration	Configuration information for the endpoint for the data source.	object This property has a sub-property called repositoryEndpointMetadata .	Yes
repositoryEndpointMetadata	This is the endpoint information for the data source. This is a sub-property for the connectionConfiguration .	object This property has a sub-property called BucketName .	Yes
BucketName	The name of your Amazon S3 bucket. This is a sub-property for the repositoryEndpointMetadata .	string	Yes
repositoryConfigurations	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings .	object This property has a sub-property called document.	Yes

Configuration	Description	Type	Required
`document`	This property has information related to the document.	`object` This property has a sub-property called `fieldMappings` .	Yes
`fieldMappings`	This property has information related to the document.	`array` This property has the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName`	Yes
`indexFieldName`	The name of the index field. This is a sub-property for the `fieldMappings` .	`string`	Yes
`indexFieldType`	The type of the index field. This is a sub-property for the `fieldMappings` .	`string` The only allowed value is `STRING`.	Yes
`dataSourceFieldName`	The field name of the data source. This is a sub-property for the `fieldMappings` .	`string`	Yes

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties that are not required • aclConfigurationFilePath • metadataFilesPrefix . • maxFileSizeInMegaBytes • inclusionPatterns • exclusionPatterns • inclusionPrefixes • exclusionPrefixes	No
aclConfigurationFilePath	The path to the file that controls access control information for your documents in an Amazon Q index. This is a sub-property of additionalProperties .	string	No

Configuration	Description	Type	Required
`metadataFilesPrefix`	The location, in your Amazon S3 bucket, of your document metadata files. This is a sub-property of `additionalProperties` .	`string`	No
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB. You can go up to 10 GB (10240 MB) if you enable **Video files** in **Multi-media content** configuration, and up to 2 GB (2048 MB) if you enable **Audio files** in **Multi-media content configuration**.	`string` You can enter a value between `0` and `10240`.	No

Configuration	Description	Type	Required
All of these following are sub-properties of `additionalProperties` • `inclusionPatterns` • `exclusionPatterns` • `inclusionPrefixes` • `exclusionPrefixes`	A list of regular expression patterns to include or exclude specific files in your Amazon S3 data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.	`array`	No
`version`	The version of the template that's supported.	`string` The default value is `1.0.0`.	No

Amazon S3 JSON schema

The following is the Amazon S3 JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "pattern": "S3"
    },
```

```
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL"]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "BucketName": {
              "type": "string"
            }
          },
          "required": ["BucketName"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "document": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    }
                  },
                  "required": [
                    "indexFieldName",
```

```
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    },
    "required": ["document"]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "inclusionPatterns": {
        "type": "array"
      },
      "exclusionPatterns": {
        "type": "array"
      },
      "inclusionPrefixes": {
        "type": "array"
      },
      "exclusionPrefixes": {
        "type": "array"
      },
      "aclConfigurationFilePath": {
        "type": "string"
      },
      "metadataFilesPrefix": {
        "type": "string"
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "enableDeletionProtection": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
```

```
            }
          ]
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      }
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "2.0.0"
      }
    ]
  },
  "required": [
    "type",
    "syncMode",
    "connectionConfiguration",
    "repositoryConfigurations"
  ]
}
```

Amazon S3 JSON schema example

The following is the Amazon S3 JSON schema example:

```
{
  "type": "S3",
  "syncMode": "FULL_CRAWL",
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "BucketName": "my-company-data-bucket"
    }
  },
  "repositoryConfigurations": {
    "document": {
      "fieldMappings": [
        {
          "dataSourceFieldName": "content",
          "indexFieldName": "document_content",
```

```
          "indexFieldType": "STRING"
        }
      ]
    }
  },
  "additionalProperties": {
    "inclusionPatterns": ["*.pdf", "*.docx"],
    "exclusionPatterns": ["*.tmp"],
    "inclusionPrefixes": ["/important-docs/"],
    "exclusionPrefixes": ["/temporary/"],
    "aclConfigurationFilePath": "/configs/acl.json",
    "metadataFilesPrefix": "/metadata/",
    "maxFileSizeInMegaBytes": "10240"

  }
}
```

Connecting Amazon Q Business to Amazon S3 using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- Amazon S3 configuration properties
- Amazon S3 JSON schema for using the configuration property with AWS CloudFormation
- Amazon S3 YAML schema for using the configuration property with AWS CloudFormation

Amazon S3 configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`type`	The type of data source. Specify S3 as your data source type.	`string` The only allowed value is S3 .	Yes
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	`string` You can choose from the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use `FULL_CRAWL` to increment ally crawl only new, modified, and deleted content each time your data source syncs with your index	Yes
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has a sub-property called `repositor`	Yes

Configuration	Description	Type	Required
		`yEndpoint Metadata .`	
`repositor yEndpoint Metadata`	This is the endpoint information for the data source. This is a sub-property for the `connectio nConfiguration .`	`object` This property has a sub-property called `BucketName .`	Yes
`BucketName`	The name of your Amazon S3 bucket. This is a sub-property for the `repositor yEndpoint Metadata .`	`string`	Yes
`repositor yConfigur ations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings .	`object` This property has a sub-property called `document.`	Yes
`document`	This property has information related to the document.	`object` This property has a sub-property called `fieldMappings .`	Yes

Configuration	Description	Type	Required
`fieldMappings`	This property has information related to the document.	`array` This property has the following sub-properties. • `indexFieldName` • `indexFieldType` • `dataSourceFieldName`	Yes
`indexFieldName`	The name of the index field. This is a sub-property for the `fieldMappings` .	`string`	Yes
`indexFieldType`	The type of the index field. This is a sub-property for the `fieldMappings` .	`string` The only allowed value is `STRING`.	Yes
`dataSourceFieldName`	The field name of the data source. This is a sub-property for the `fieldMappings` .	`string`	Yes

Configuration	Description	Type	Required
`additionalProperties`	Additional configuration options for your content in your data source.	`object` This property has the following sub-properties that are not required • `aclConfigurationFilePath` • `metadataFilesPrefix` . • `maxFileSizeInMegaBytes` • `inclusionPatterns` • `exclusionPatterns` • `inclusionPrefixes` • `exclusionPrefixes`	No
`aclConfigurationFilePath`	The path to the file that controls access control information for your documents in an Amazon Q index. This is a sub-property of `additionalProperties` .	`string`	No

Configuration	Description	Type	Required
`metadataFilesPrefix`	The location, in your Amazon S3 bucket, of your document metadata files. This is a sub-property of `additionalProperties` .	`string`	No
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB. You can go up to 10 GB (10240 MB) if you enable **Video files** in **Multi-media content** configuration, and up to 2 GB (2048 MB) if you enable **Audio files** in **Multi-media content configuration**.	`string` You can enter a value between `0` and `10240`.	No

Configuration	Description	Type	Required
All of these following are sub-properties of `additionalProperties` • `inclusionPatterns` • `exclusionPatterns` • `inclusionPrefixes` • `exclusionPrefixes`	A list of regular expression patterns to include or exclude specific files in your Amazon S3 data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.	`array`	No
`version`	The version of the template that's supported.	`string` The default value is `1.0.0`.	No

Amazon S3 JSON schema for using the configuration property with AWS CloudFormation

The following is the Amazon S3 JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- Amazon S3 JSON schema for using the configuration property with AWS CloudFormation
- Amazon S3 JSON schema example for using the configuration property with AWS CloudFormation

Amazon S3 JSON schema for using the configuration property with AWS CloudFormation

The following is the Amazon S3 JSON schema for the configuration property for CloudFormation.

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "pattern": "S3"
    },
    "syncMode": {
      "type": "string",
      "enum": ["FULL_CRAWL", "FORCED_FULL_CRAWL"]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "BucketName": {
              "type": "string"
            }
          },
          "required": ["BucketName"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "document": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
```

```
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        }
      },
      "required": ["document"]
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "inclusionPatterns": {
          "type": "array"
        },
        "exclusionPatterns": {
          "type": "array"
        },
        "inclusionPrefixes": {
          "type": "array"
        },
        "exclusionPrefixes": {
          "type": "array"
        },
        "aclConfigurationFilePath": {
          "type": "string"
        },
        "metadataFilesPrefix": {
          "type": "string"
        },
```

```
        "maxFileSizeInMegaBytes": {
          "type": "string"
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      }
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "type",
    "syncMode",
    "connectionConfiguration",
    "repositoryConfigurations"
  ]
}
```

Amazon S3 JSON schema example for using the configuration property with AWS CloudFormation

The following is the Amazon S3 JSON example for the Configuration property for CloudFormation.

```
{
```

```
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation Amazon S3 Data Source Template",
  "Resources": {
    "DataSourceS3": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MyS3DataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "S3",
          "syncMode": "FULL_CRAWL",
          "connectionConfiguration": {
            "repositoryEndpointMetadata": {
              "BucketName": "my-company-data-bucket"
            }
          },
          "repositoryConfigurations": {
            "document": {
              "fieldMappings": [
                {
                  "dataSourceFieldName": "content",
                  "indexFieldName": "document_content",
                  "indexFieldType": "STRING"
                }
              ]
            }
          },
          "additionalProperties": {
            "inclusionPatterns": ["*.pdf", "*.docx"],
            "exclusionPatterns": ["*.tmp"],
            "inclusionPrefixes": ["/important-docs/"],
            "exclusionPrefixes": ["/temporary/"],
            "aclConfigurationFilePath": "/configs/acl.json",
            "metadataFilesPrefix": "/metadata/",
            "maxFileSizeInMegaBytes": "50"
          }
        }
      }
    }
  }
}
```

Amazon S3 YAML schema for using the configuration property with AWS CloudFormation

The following is the Amazon S3 YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- Amazon S3 YAML schema for using the configuration property with AWS CloudFormation
- Amazon S3 YAML schema example for using the configuration property with AWS CloudFormation

Amazon S3 YAML schema for using the configuration property with AWS CloudFormation

The following is the Amazon S3 YAML schema for the configuration property for CloudFormation.

```
type: object
properties:
  type:
    type: string
    pattern: S3
  syncMode:
    type: string
    enum:
      - FULL_CRAWL
      - FORCED_FULL_CRAWL
  connectionConfiguration:
    type: object
    properties:
      repositoryEndpointMetadata:
        type: object
        properties:
          BucketName:
            type: string
        required:
          - BucketName
    required:
      - repositoryEndpointMetadata
  repositoryConfigurations:
    type: object
    properties:
      document:
        type: object
        properties:
```

```
          fieldMappings:
            type: array
            items:
              - type: object
                properties:
                  indexFieldName:
                    type: string
                  indexFieldType:
                    type: string
                    enum:
                      - STRING
                  dataSourceFieldName:
                    type: string
                required:
                  - indexFieldName
                  - indexFieldType
                  - dataSourceFieldName
        required:
          - fieldMappings
    required:
      - document
  additionalProperties:
    type: object
    properties:
      inclusionPatterns:
        type: array
      exclusionPatterns:
        type: array
      inclusionPrefixes:
        type: array
      exclusionPrefixes:
        type: array
      aclConfigurationFilePath:
        type: string
      metadataFilesPrefix:
        type: string
      maxFileSizeInMegaBytes:
        type: string
      enableDeletionProtection:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
```

```
              - "false"
      deletionProtectionThreshold:
        type: string
        default: "15"
version:
  type: string
  anyOf:
    - pattern: 1.0.0
required:
  - type
  - syncMode
  - connectionConfiguration
  - repositoryConfigurations
```

Amazon S3 YAML schema example for using the configuration property with AWS CloudFormation

The following is the Amazon S3 YAML example for the Configuration property for CloudFormation:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: "CloudFormation Amazon S3 Data Source Template"
Resources:
  DataSourceS3:
    Type: "AWS::QBusiness::DataSource"
    Properties:
      ApplicationId: app12345-1234-1234-1234-123456789012
      IndexId: indx1234-1234-1234-1234-123456789012
      DisplayName: MyS3DataSource
      RoleArn: arn:aws:iam::123456789012:role/qbusiness-data-source-role
      Configuration:
        type: S3
        syncMode: FULL_CRAWL
        connectionConfiguration:
          repositoryEndpointMetadata:
            BucketName: my-company-data-bucket
        repositoryConfigurations:
          document:
            fieldMappings:
              - dataSourceFieldName: content
                indexFieldName: document_content
                indexFieldType: STRING
        additionalProperties:
          inclusionPatterns:
```

```
      - "*.pdf"
      - "*.docx"
    exclusionPatterns:
      - "*.tmp"
    inclusionPrefixes:
      - "/important-docs/"
    exclusionPrefixes:
      - "/temporary/"
    aclConfigurationFilePath: "/configs/acl.json"
    metadataFilesPrefix: "/metadata/"
    maxFileSizeInMegaBytes: "50"
```

IAM role

Whether you use the AWS Management Console or the CreateDataSource API, you must provide an IAM role that allows Amazon Q Business to access your Amazon S3 bucket.

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q Business resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role while creating your data source.

> **Note**
>
> To learn how to create an IAM role, see Create a role to delegate permissions to an AWS service.

Cross-account Amazon S3 buckets are supported with Amazon Q Business. However, your bucket must be located in the same AWS Region as your Amazon Q Business index, and your index must have permissions to access the bucket containing your documents.

When you use an Amazon S3 bucket as a data source, you must provide a role that has permissions to:

- Access your Amazon S3 bucket.
- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` API operations in order to ingest documents.

- Permission to access the Principal Store APIs needed to ingest access control and identity information from documents.

Cross-account Amazon S3 buckets are supported. To configure cross-account Amazon S3 bucket access, follow these steps:

Configuring Cross-Account Amazon S3 Permissions

1. **Data Source Inline Policy** - Navigate to the IAM console, select the Role used for the data source, and click on "Create inline policy." Use the following JSON policy:

```
{
"Version": "2012-10-17",       ,
"Statement": [
  {
    "Sid": "AllowsAmazonQToGetObjectfromS3",
    "Action": [
      "s3:GetObject"
    ],
    "Resource": [
      "arn:aws:s3:::<Bucket Name Here>/*"
    ],
    "Effect": "Allow",
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "<Cross Account AWS Account ID Here>"
      }
    }
  },
  {
    "Sid": "AllowsAmazonQToListS3Buckets",
    "Action": [
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::<Bucket Name Here>"
    ],
    "Effect": "Allow",
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "<Cross Account AWS Account ID Here>"
      }
```

```
    }
  },
  {
    "Sid": "AllowsAmazonQToIngestDocuments",
    "Effect": "Allow",
    "Action": [
      "qbusiness:BatchPutDocument",
      "qbusiness:BatchDeleteDocument"
    ],
    "Resource": "<Amazon Q Business Index ARN Here>"
  },
  {
    "Sid": "AllowsAmazonQToCallPrincipalMappingAPIs",
    "Effect": "Allow",
    "Action": [
      "qbusiness:PutGroup",
      "qbusiness:CreateUser",
      "qbusiness:DeleteGroup",
      "qbusiness:UpdateUser",
      "qbusiness:ListGroups"
    ],
    "Resource": [
      "<Amazon Q Business Application ARN Here>",
      "<Amazon Q Business Index ARN Here>",
      "<Amazon Q Business Index ARN Here>/data-source/*"
    ]
  }
]
}
```

2. **Amazon S3 Bucket Policy** - Attach the following policy to the Amazon S3 bucket policy:

```
{
"Version": "2012-10-17",       ,
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "$amazonq-s3-connector-role-arn"
    },
    "Action": [
      "s3:GetObject"
    ],
    "Resource": [
```

```
      "arn:aws:s3:::$bucket-in-other-account/*"
    ]
  },
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "$amazonq-s3-connector-role-arn"
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::$bucket-in-other-account"
  }
]
}
```

To allow Amazon Q to use an Amazon S3 bucket as a data source, use the following role policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetObjectfromS3",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::{{input_bucket_name}}/*"
      ],
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "{{account_id}}"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToListS3Buckets",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::{{input_bucket_name}}"
      ],
```

```
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "{{account_id}}"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
    },
    {
      "Sid": "AllowsAmazonQToCallPrincipalMappingAPIs",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToPassCustomerRole",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::{{account_id}}:role/QBusiness-DataSource-*"
      ],
```

```
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "qbusiness.amazonaws.com"
        }
      }
    }
  ]
}
```

If the documents in the Amazon S3 bucket are encrypted, you must provide the following permissions to use the AWS KMS key to decrypt the documents:

```
{
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    }
```

If you are using an Amazon VPC, you must add the following VPC access permissions to your policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetObjectfromS3",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::{{input_bucket_name}}/*"
```

```
      ],
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "{{account_id}}"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToListS3Buckets",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::{{input_bucket_name}}"
      ],
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "{{account_id}}"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/{{index_id}}"
    },
    {
      "Sid": "AllowsAmazonQToCallPrincipalMappingAPIs",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
```

```
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteENI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateDeleteENI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
```

```
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToConnectToVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
```

```
      "Sid": "AllowsAmazonQToAssumeRoleForServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

Amazon S3 data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

Important

Filtering using document attributes in chat is only supported through the API.

The Amazon Q Amazon S3 connector supports the following entities and the associated reserved and custom attributes.

Supported entities and field mappings

- Document

Document

Amazon S3 field name	Index field name	Description	Data type
s3_document_id	s3_document_id	Default	String

Clickable URLs

The Clickable URL feature allows end users to access source documents through citation links in chat responses, regardless of whether a source URI is configured.

This feature improves the verification experience by making all documents of supported datasource types accessible. Currently, clickable links are only supported for Amazon S3, custom connectors, file upload and direct `BatchPutDocument` ingestion of documents.

Configuration Requirements: While this feature works automatically for new applications, existing customers may need additional configuration:

- If you already use Amazon S3 data source for your Amazon Q Business application, you will need to perform a full sync of the data source for the clickable URLs feature to be available to your users.
- If you already use an Amazon Q Business web experience, you may need to add additional permissions to the IAM role for the web experience. See the troubleshooting section below for details.

Download Concurrency Limit: For information about file size limits, see Quotas and regions.

Access Control: The Clickable URL respects all access control settings:

- If a user's access to a file is revoked after they've viewed it in a chat, once a resync is performed subsequent attempts to access the file will be denied with a clear error message.
- If a file is updated after a chat reference, then once a resync is performed clicking the link will retrieve the current version of the file.
- If a file is deleted and a resync is performed users will receive a clear error message indicating the file no longer exists.

Troubleshooting clickable links

This section helps you resolve errors that you might encounter when using clickable links for source references in your conversations with your Amazon Q Business AI assistant.

Full sync required

> **Note**
>
> The following suggested troubleshooting steps apply only to existing accounts using the Amazon S3 connector.

Issue: When you try to access referenced URLs from an Amazon S3 or uploaded files data source, you receive the following error message.

Error message:

```
This document cannot be downloaded because the raw document download feature requires a
 full connector sync performed after 07/02/2025. Your admin has not yet completed this
 full sync. Please contact your admin to request a complete sync of the data source.
```

Solution: This error occurs when the data source hasn't completed a full sync after the clickable links feature was enabled. To resolve this issue:

- For S3 data sources: Perform a full sync of the S3 data source.
- For uploaded files data sources: Delete the files from the upload files data source and upload them again.

Permission changes

Issue: When browsing conversation history, you click on a reference URL from an Amazon S3 data source but can't view or download the file.

Error message:

```
You no longer have permission to access this document. The access permissions for this
 document have been changed since you last accessed it. Please contact your admin if
 you believe you should have access to this content.
```

Solution: This error occurs when the permissions for the document in the ACLs on the Amazon S3 bucket changed after your conversation, removing your access to the file. The ACLs were updated in the Amazon Q Business index during a subsequent data source sync. If you believe you should have access to the document, contact your administrator to:

- Review and update the ACLs
- Perform a data source sync

Document not found

Issue: When browsing conversation history, you click on a reference URL from an Amazon S3 or upload files data source but can't view or download the file.

Error message:

```
The document you're trying to access no longer exists in the data source. It may have
 been deleted or moved since it was last referenced. Please check with the admin if you
 need access to this document.
```

Solution: This error occurs when the document was deleted from the Amazon S3 bucket, moved to a different location, or deleted from the upload files data source after your conversation. The document was also removed from the Amazon Q Business index and staging bucket during a subsequent data source sync. If you believe the document shouldn't have been deleted, contact your administrator to restore the document and perform a data source sync.

Insufficient permissions

> **Note**
>
> The following suggested troubleshooting steps apply only to existing accounts using the Amazon S3 connector.

Issue: When you click on a reference URL from an Amazon S3 or upload files data source, you can't view or download the file.

Error message:

```
Unable to download this document because your Web Experience lacks the required
 permissions. Your admin needs to update the IAM role for the Web Experience to include
 permissions for the GetDocumentContent API. Please contact your admin to request this
 IAM role update.
```

Solution: This error occurs when the web experience doesn't have the required permissions to invoke the GetDocumentContent API. Your administrator can resolve this error by updating the IAM role for the web experience with the permissions described in the *Considerations for using S3 clickable URLs* section.

If you already use a Amazon Q Business web experience, add the following permissions to the IAM role for the Amazon Q Business web experience:

```
{
    "Sid": "QBusinessGetDocumentContentPermission",
    "Effect": "Allow",
    "Action": ["qbusiness:GetDocumentContent"],
    "Resource": [
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{source_account}}:application/
{{application_id}}/index/*"
    ]
}
```

Adding document metadata in Amazon S3

To customize chat results for your end users, you can add metadata or document attributes to documents in an Amazon S3 bucket by using a metadata file. Metadata is additional information about a document, such as its title and the date and time it was created. To learn more about metadata in Amazon Q Business, see Document attributes in Amazon Q Business.

Amazon Q Business supports source attribution with citations. If you specify the `_source_uri` metadata field when you add metadata to your Amazon S3 bucket, the source attribution links returned by Amazon Q Business in the chat results will direct users to the configured URL. If you don't specify a `_source_uri`, users can still access the source documents through clickable citation links that will download the file at query time. This allows users to verify information even when no source URI is configured.

Topics

- Document metadata location
- Document metadata structure

Document metadata location

In Amazon S3, each metadata file can be associated with an indexed document. Your metadata files must be stored in the same Amazon S3 bucket as your indexed files. You can specify a location within the Amazon S3 bucket for your metadata files by using the AWS Management Console. Or, you can use the `metadataFilesPrefix` field of the Amazon S3 `configuration` parameter using the JSON schema when you create an Amazon S3 data source using the CreateDataSource API.

If you don't specify an Amazon S3 prefix, your metadata files must be stored in the same location as your indexed documents. If you specify an Amazon S3 prefix for your metadata files, they must be in a directory structure parallel to your indexed documents. Amazon Q looks only in the specified directory for your metadata. If the metadata isn't read, check that the directory location matches the location of your metadata.

The following examples show how the indexed document location maps to the metadata file location. The document's Amazon S3 key is appended to the metadata's Amazon S3 prefix and then suffixed with `.metadata.json` to form the metadata file's Amazon S3 path.

> **Note**
>
> The combined Amazon S3 key, the metadata's Amazon S3 prefix, and the `.metadata.json` suffix must be no more than a total of 1,024 characters. We recommend that your Amazon S3 key is less than 1,000 characters to account for additional characters when combining your key with the prefix and suffix.

```
Bucket name:
     s3://bucketName
Document path:
     documents
Metadata path:
     none
File mapping
     s3://bucketName/documents/file.txt ->
        s3://bucketName/documents/file.txt.metadata.json
```

```
Bucket name:
     s3://bucketName
Document path:
     documents/legal
Metadata path:
     metadata
File mapping
     s3://bucketName/documents/legal/file.txt ->
        s3://bucketName/metadata/documents/legal/file.txt.metadata.json
```

Document metadata structure

You define your document metadata itself in a JSON file. The file must be a UTF-8 text file without a BOM marker. The file name of the JSON file must be <*document*>.<*extension*>.metadata.json. In this example, *document* is the name of the document that the metadata applies to and *extension* is the file extension for the document. The document ID must be unique in <*document*>.<*extension*>.metadata.json.

The content of the JSON file uses the following template:

```
{
    "DocumentId": "document ID",
```

```
    "Attributes": {
        "_category": "document category",
        "_created_at": "ISO 8601 encoded string",
        "_last_updated_at": "ISO 8601 encoded string",
        "_source_uri": "document URI",
        "_version": "file version",
        "_view_count": number of times document has been viewed,
        "custom attribute key": "custom attribute value",
        additional custom attributes
    },
    "AccessControlList": [
         {
             "Name": "user name",
             "Type": "GROUP | USER",
             "Access": "ALLOW | DENY"
         }
    ],
    "Title": "document title",
    "ContentType": "PDF | HTML | MS_WORD | PLAIN_TEXT | PPT | RTF | XML | XSLT
 | MS_EXCEL | CSV | JSON | MD"
}
```

If you provide a Metadata path, make sure that directory structure inside the metadata directory exactly matches the directory structure of data file.

For example, if the data file location is at `s3://bucketName/documents/legal/file.txt`, the metadata file location should be at `s3://bucketName/metadata/documents/legal/file.txt.metadata.json`.

All of the attributes and fields are optional, so it's not necessary to include all attributes. However, you must provide a value for each attribute that you want to include; the value can't be empty.

The `_created_at` and `_last_updated_at` metadata fields are ISO 8601 encoded dates. For example, 2012-03-25T12:30:10+01:00 is the ISO 8601 date-time format for March 25, 2012, at 12:30PM (plus 10 seconds) in the Central European Time time zone.

You can use the `AccessControlList` field to filter the response from a query. This way, only certain users and groups have access to documents.

How Amazon Q Business connector crawls Amazon S3 ACLs

You add access control information to a document in an Amazon S3 data source using a metadata file associated with the document. You specify the file using the console or as

the `aclConfigurationFilePath` parameter when you call the `CreateDataSource` or `UpdateDataSource` API and use the `configuration` parameter.

> **Note**
>
> The ACL file and data should be stored in the same Amazon S3 bucket.

The configuration file contains a JSON structure that identifies an Amazon S3 prefix and lists the access settings for the prefix. The prefix can be a path, or it can be an individual file. If the prefix is a path, the access settings apply to all of the files in that path.

You provide three pieces of information in the file:

- The access that the entity should have. You can use `ALLOW` or `DENY`.
- The type of entity. You can use `USER` or `GROUP`.
- The name of the entity.

> **Important**
>
> The system grants ALL users access to prefixes that do NOT appear in the ACL file.

The JSON structure for the configuration file must be in the following format:

```
[
    {
        "keyPrefix": "s3://BUCKETNAME/prefix1/",
        "aclEntries": [
            {
                "Name": "user1@example.com",
                "Type": "USER",
                "Access": "ALLOW"
            },
            {
                "Name": "group1",
                "Type": "GROUP",
                "Access": "DENY"
            }
```

```
        ]
    },
    {
        "keyPrefix": "s3://BUCKETNAME/prefix2/",
        "aclEntries": [
            {
                "Name": "user2@example.com",
                "Type": "USER",
                "Access": "ALLOW"
            },
            {
                "Name": "user1@example.com",
                "Type": "USER",
                "Access": "DENY"
            },
            {
                "Name": "group1",
                "Type": "GROUP",
                "Access": "DENY"
            }
        ]
    }
]
```

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Understand error codes in the Amazon S3 connector

The following table provides information about error codes you may see for the Amazon S3 connector and suggested resolutions.

Error code	Error message	Suggested resolution
S3-5001	Profile name cannot be null or empty. Try again with a valid profile name.	Provide a valid profile name in the configuration.

Error code	Error message	Suggested resolution
S3-5002	Default AWS profile was not found. Verify the credentials file and try again.	Configure the AWS profile in the environment using "aws configure" command.
S3-5100	Bucket cannot be null or empty. Try again with a valid bucket.	Provide a valid bucket name in configuration.
S3-5101	The bucket does not exist, or it is from another region. Try again with a valid bucket.	Provide a valid bucket name that exists in the same region as the profile that is configured in the environment.
S3-5102	The ACL file is not found in the given path. Verify and try again.	Provide a valid ACL file location in configuration.
S3-5103	The ACL file reading was unsuccessful due to malformed JSON content. Verify and try again.	Verify the content of ACL file. It could contain malformed JSON content.
S3-5104	Metadata file contained malformed JSON content.	Verify content of metadata files. It could contain malformed JSON content.
S3-5105	IndexFieldName cannot be null or empty.	IndexFieldName in Field Mappings should not be null or empty.
S3-5106	IndexFieldType cannot be null or empty.	IndexFieldType in Field Mappings should not be null or empty.
S3-5107	DataSourceFieldName cannot be null or empty.	DataSourceFieldName in Field Mappings should not be null or empty.

Error code	Error message	Suggested resolution
S3-5108	Only String, String List, Date and Long formats are supported for field mappings.	IndexFieldType in field mapping could contain an unsupported type. Verify field mappings and try again.
S3-5110	Unable to connect with provided Amazon S3 bucket.	Try again with valid bucket.
S3-5111	Unable to connect with provided Amazon S3 bucket due to connection timeout.	Check if the provided bucket is valid, credentials are valid, an IAM role with correct permissions has been provided, or if the VPC configuration of the data source is correct.
S3-5200	Object was not accessibl e. Amazon S3 returned following error:	The object might be not accessible. User may receive this error if an object is encrypted using an SSE-KMS key that the profile doesn't have the access.
S3-5201	The object content was not readable. S3 returned following error:	User may receive this error if an object is encrypted using an SSE-C key.

Connecting Salesforce Online to Amazon Q Business

Salesforce is a customer relationship management (CRM) tool for managing support, sales, and marketing teams. You can connect Salesforce Online instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

The Amazon Q Salesforce Online connector supports the following Salesforce Online editions: Developer Edition and Enterprise Edition.

Topics

- Known limitations for the Salesforce Online connector

- Salesforce Online connector overview
- Prerequisites for connecting Amazon Q Business to Salesforce Online
- Setting up Salesforce Online for connecting to Amazon Q Business
- Connecting Amazon Q Business to Salesforce Online using the console
- Connecting Amazon Q Business to Salesforce using APIs
- How Amazon Q Business connector crawls Salesforce ACLs
- Salesforce Online data source connector field mappings
- IAM role for Salesforce Online connector
- Troubleshooting your Salesforce Online connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Salesforce Online connector

The Salesforce Online connector has the following known limitations:

- The Salesforce Online connector doesn't currently (as of 2/14/25) support explicit deny permission specifications for Contract, Task, and Custom objects and their respective attachments, although it respects base access controls for Salesforce Online entities. Users who have access to an entity through base access controls would still have access to those entities in Amazon Q Business - even if they have been added to the explicit deny list in Salesforce.
- The Salesforce Online connector doesn't support field-level access control, respecting only the parent-level access control. If a field-level access control configuration is detected within an entity, Amazon Q Business will utilize the parent level security setting. This means that if a user has access to the parent entity/document in Salesforce, they will be able to see all fields of that document in Amazon Q Business, regardless of any field-level security restrictions that exist in Salesforce.

- The Salesforce Online connector does not offer the ability to perform incremental syncs based on new, modified, or deleted files. At this time, it can perform only full syncs.
- The Salesforce Online API doesn't provide the status of deleted **Group**, **Partner**, **Profile**, and **User** entities. So, the Salesforce Online connector can't retrieve this information.
- The Salesforce Online API doesn't provide the status of modified **Attachment titles** (Lightning Version). So, the Salesforce Online connector can't retrieve this information.
- The Salesforce Online connector supports custom field mappings only for the following entities: **Account**, **Campaign**, **Contact**, **Contract**, **Case**, **Product Lead**, **Pricebook**, and **CustomEntity**.
- The Salesforce Online API does not provide ACL information for documents with shared access types.
- By default, Salesforce Online Developer has a maximum limit of 15000 total calls per 24 hour period. If a request exceeds this limit, the API returns a `REQUEST_LIMIT_EXCEEDED` error.
- Because Amazon Q Business uses email address as unique identifiers, each user must have a unique email address.
- The Salesforce Online connector only updates user status during connector syncs, meaning that any deactivated users are only deactivated in Amazon Q Business during the next connector sync. If a user is deactivated in Salesforce they may retain access through Amazon Q Business until the next sync.
- The Salesforce Online connector respects hierarchies for custom object record access regardless of Salesforce settings, due to Salesforce API limitations. In other words, while Salesforce Online lets users disable Grant Access Using Hierarchies for custom objects, the role hierarchy will still apply for Amazon Q Business.
- When Access Control Lists (ACLs) are enabled, the "Sync only new or modified content" option is not available due to Salesforce Online API limitations. We recommend using "Full sync" or "New, modified, or deleted content sync" modes instead, or disable ACLs if you need to use this sync mode.

Salesforce Online connector overview

The following table gives an overview of the Salesforce Online connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	OAuth 2.0 with Resource Owner Password Flow Note that Require Proof Key for Code Exchange (PKCE) is not supported and must be disabled.
	Authentication credentials	• Salesforce authentication URL • Username Client secret • Password username • Security token • Consumer key • Consumer secret
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes
	Supported versions	• API 30-56 • Lightning, Classic • Sandbox
Crawl features	**Custom objects**	Yes
	Custom metadata	Yes
	Entities	Yes. The following entities are supported: • Account • Campaign • Partner • Pricebook • Case • Contact

Category	Feature	Support
		• Contract • Document • Group • Idea • Lead • Opportunity • Product • Profile • Solution • Task • User • Chatter • Knowledge Articles See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.
	Filters	Yes. The following filters are supported: • Attachment filter for supported entities • Regex filters for entities • Inclusion and exclusion filters on file type for Documents • Inclusion and exclusion filters on File Name and File Type for Attachments

Category	Feature	Support
	Sync mode	Supports incremental sync only if ACL is turned off, otherwise only full sync will be used.
	File types	Supports all files supported by Amazon Q.
	Crawled as a document	• Each account • Each contact • Each campaign • Each contract • Each case • Each partner • Each opportunity • Each group • Each lead • Each user • Each task • Each idea • Each profile • Each solution • Each chatter • Each document • Each custom entity • Each knowledge article

Prerequisites for connecting Amazon Q Business to Salesforce Online

Before you begin, make sure that you have completed the following prerequisites.

In Salesforce, make sure you have:

- Copied the Salesforce security token associated with the account that's used to connect to Salesforce.
- Created a Salesforce Connected App account with OAuth activated and have copied the consumer key (client ID) and consumer secret (client secret) assigned to your Salesforce Connected App. For more information, see Salesforce documentation on Connected Apps on the Salesforce website.
- Copied the URL of the Salesforce instance that you want to index. Typically, this is *https://<company>.salesforce.com/*. The server must be running a Salesforce connected app.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Salesforce Online authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Setting up Salesforce Online for connecting to Amazon Q Business

Before you connect Salesforce Online to Amazon Q Business, you need to create and retrieve the Salesforce Online credentials you will use to connect Salesforce Online to Amazon Q. You will also need to add any authorization permissions needed by Salesforce Online to connect to Amazon Q.

The following procedure gives you an overview of how to configure Salesforce Online for Amazon Q.

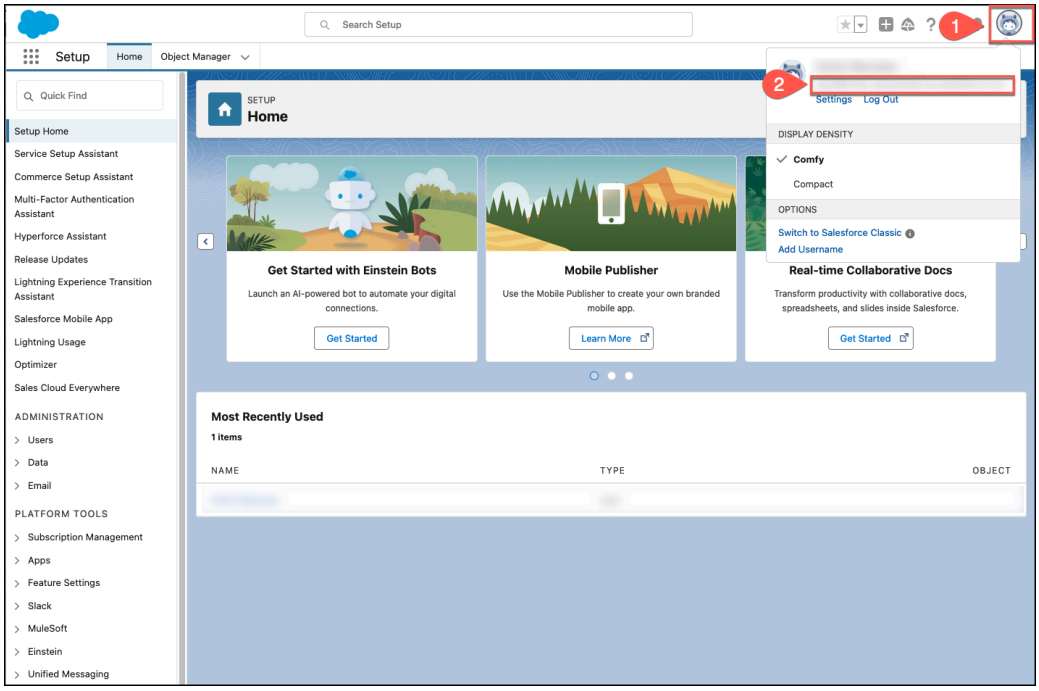
Configuring Salesforce Online for Amazon Q

1. Create a Salesforce Online instance at https://developer.salesforce.com/signup. Note the username and password you logged in with. Also note the Salesforce Online URL that's sent to your email on successful instance setup.

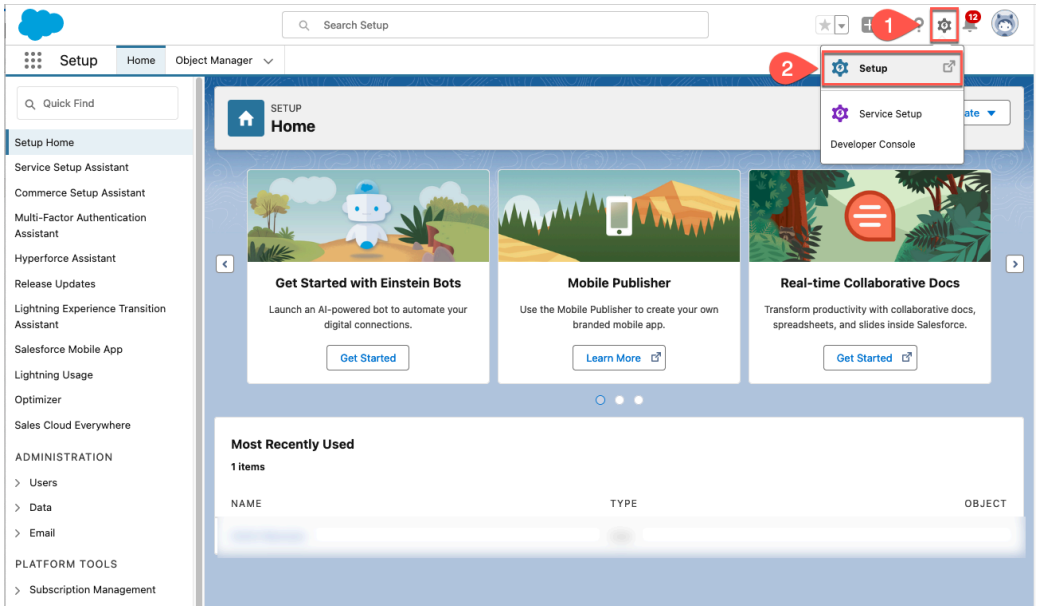
   You will need these pieces of information later to connect to Amazon Q.

2. Log in to your Salesforce Online Developer Edition account at https://login.salesforce.com or Salesforce Online Sandbox Edition account at https://test.salesforce.com.

3. From the Salesforce Online profile menu, copy your Salesforce Online URL, if you haven't already. This will be the URL you will input as host URL in Amazon Q.

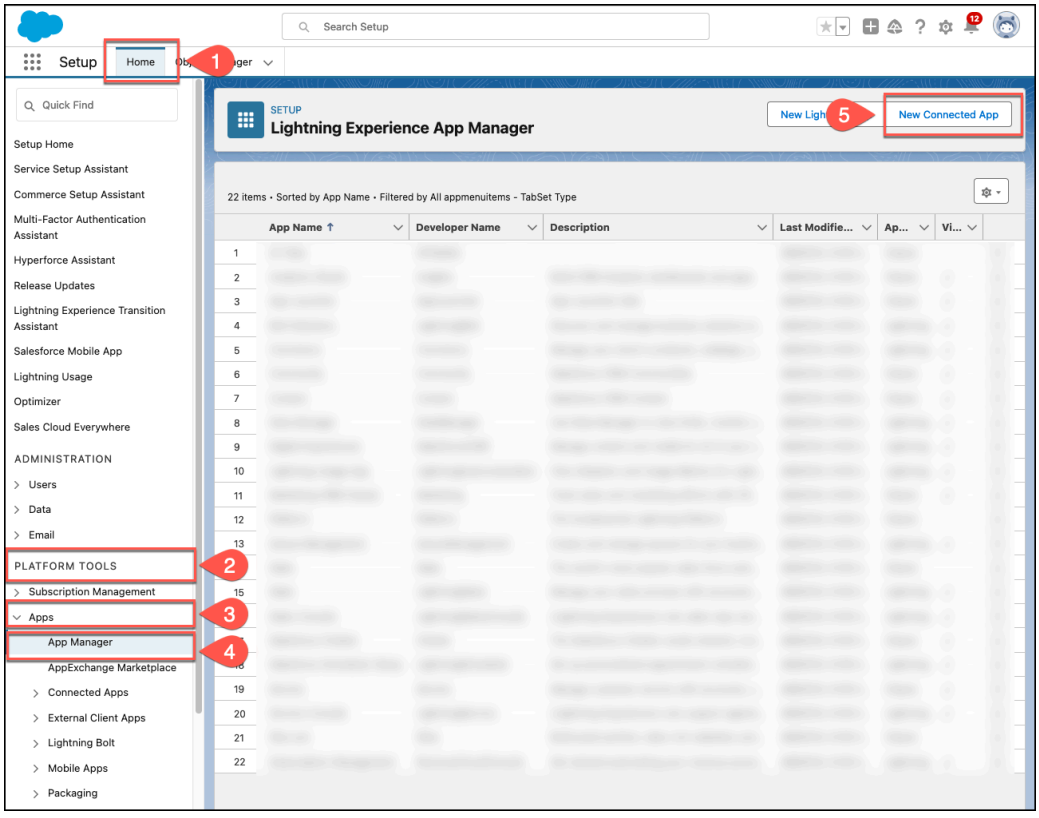


4. Then, from the Salesforce Online profile menu, select the **Setup** icon and then select **Setup**.



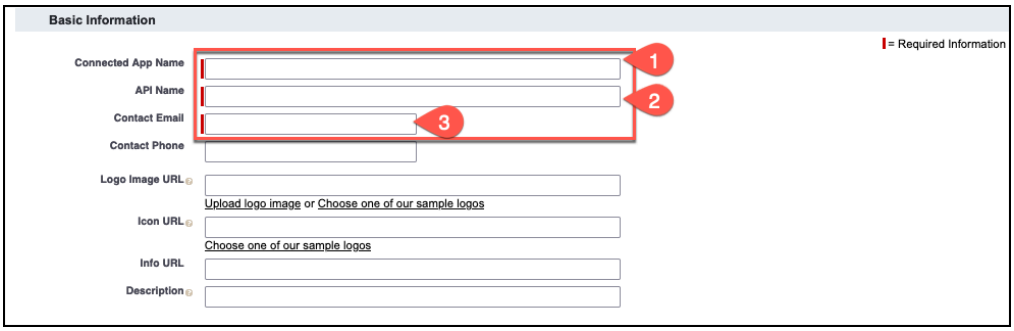
5. From the left navigation menu, on the **Setup** home page, go to **Platform tools**, select **Apps**, and then, select **App manager**.

   Then, from the **Lightning Experience App Manager** page, select **New Connected App**.



6. On the **New Connected App** page, do the following:

- In **Basic information**, enter the following required information:
  - **Connect App Name** – A name for your connected app.
  - **API Name** – A name for your API.
  - **Contact Email** – Your contact email.



  Enter other values as per your use case.

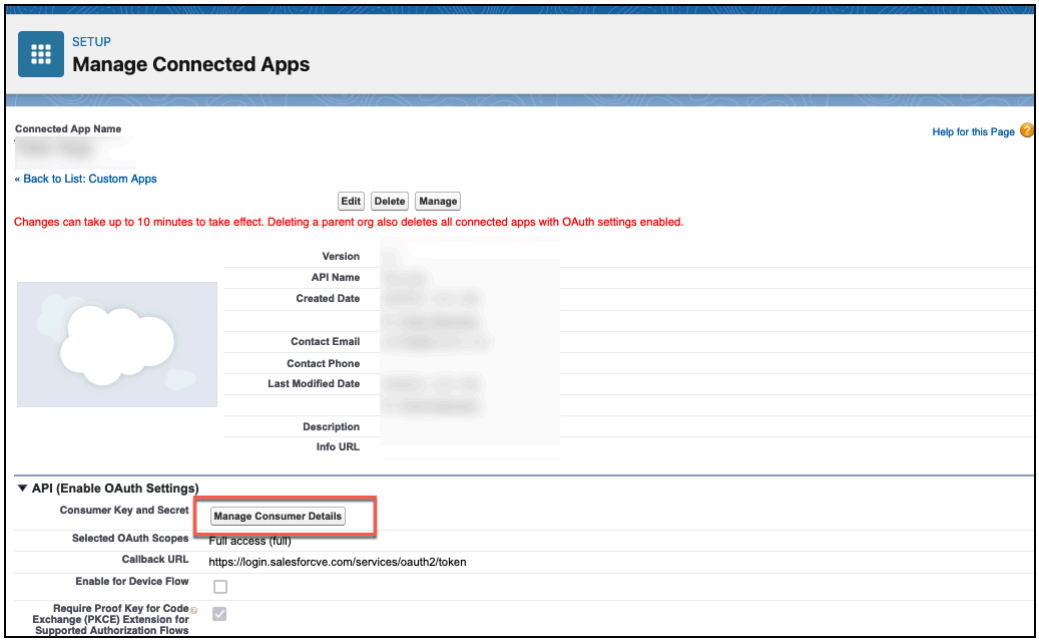
- In **API (Enable OAuth Settings)**, select the checkbox to enable. Then, enter the following information:
  - **Callback URL** – Enter the following callback URL, depending on your Salesforce Online account type:
    - Developer Edition – `https://login.salesforce.com/services/oauth2/token`
    - Sandbox Edition – `https://test.salesforce.com/services/oauth2/token`

    Also, copy and save this URL in a text editor of your choice. You will enter this callback URL in Amazon Q later as **Authentication URL**.
  - **Select OAuth Scopes** – Select **Full access (full)** as your OAuth Scope.
  - **Introspect All Tokens** – Select this option to generate access tokens in a future step. You need this access token to connect to Amazon Q. You enter this as the **Security token** in the Amazon Q console.

  Select other options as per your use case.

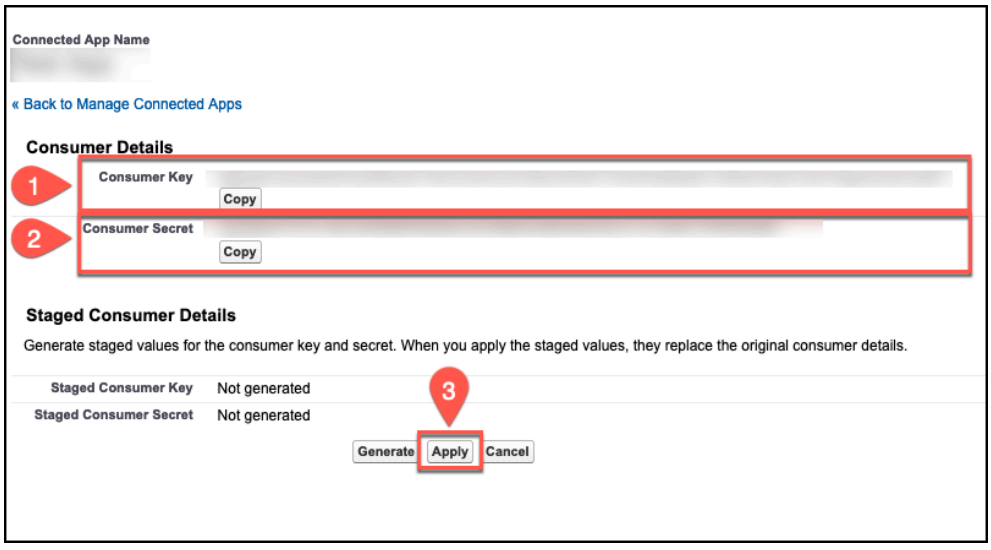
- Select **Save**.

7. From the **Manage Connected Apps** page that opens, choose **Manage Consumer Details**. You will be redirected to a **Connected App Name** summary page.

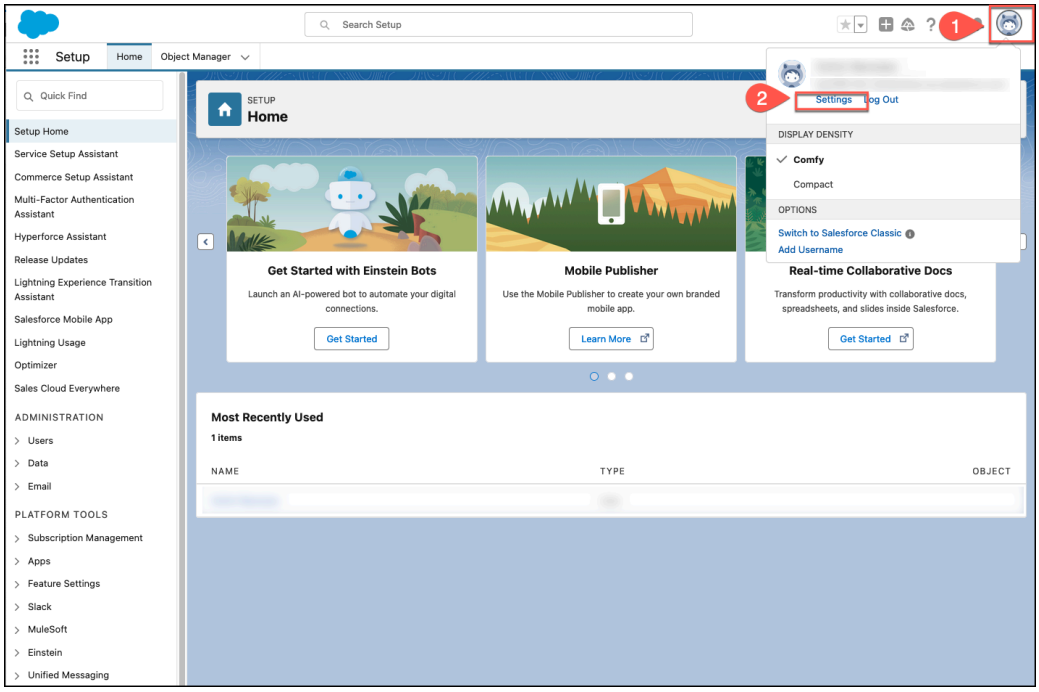


8. On the **Connected App Name** page, do the following:

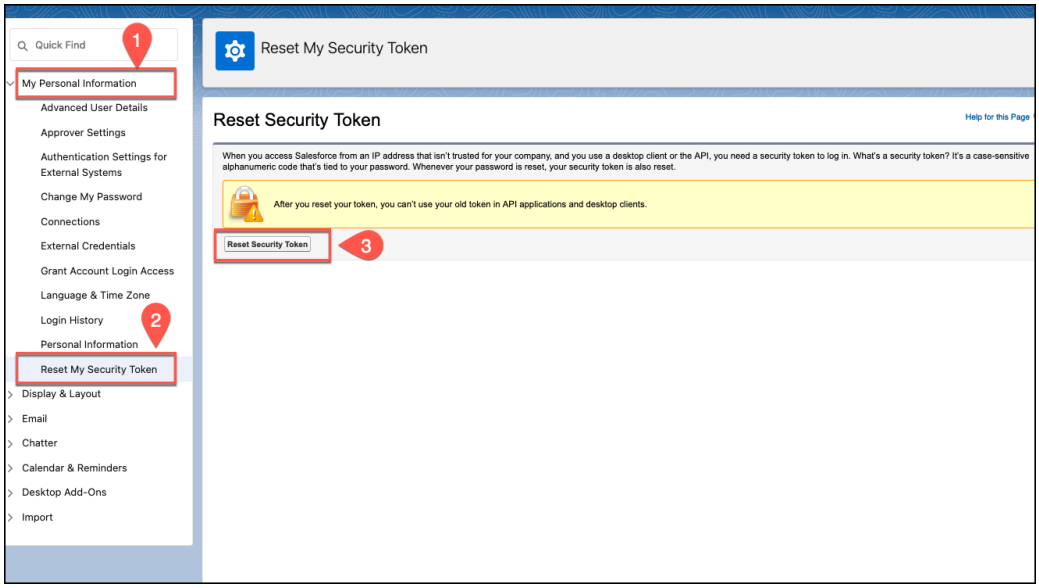
   - From **Consumer Details**, copy and save the following in a text editor of your choice:
     - **Consumer Key** – You will need this to connect Salesforce Online to Amazon Q.
     - **Consumer Secret** – You will need this to connect Salesforce Online to Amazon Q.
     - Select **Apply**.



9. Next, you will generate a security token. Navigate back to your Salesforce Online account home page. From the Salesforce Online profile menu, select **Settings**.

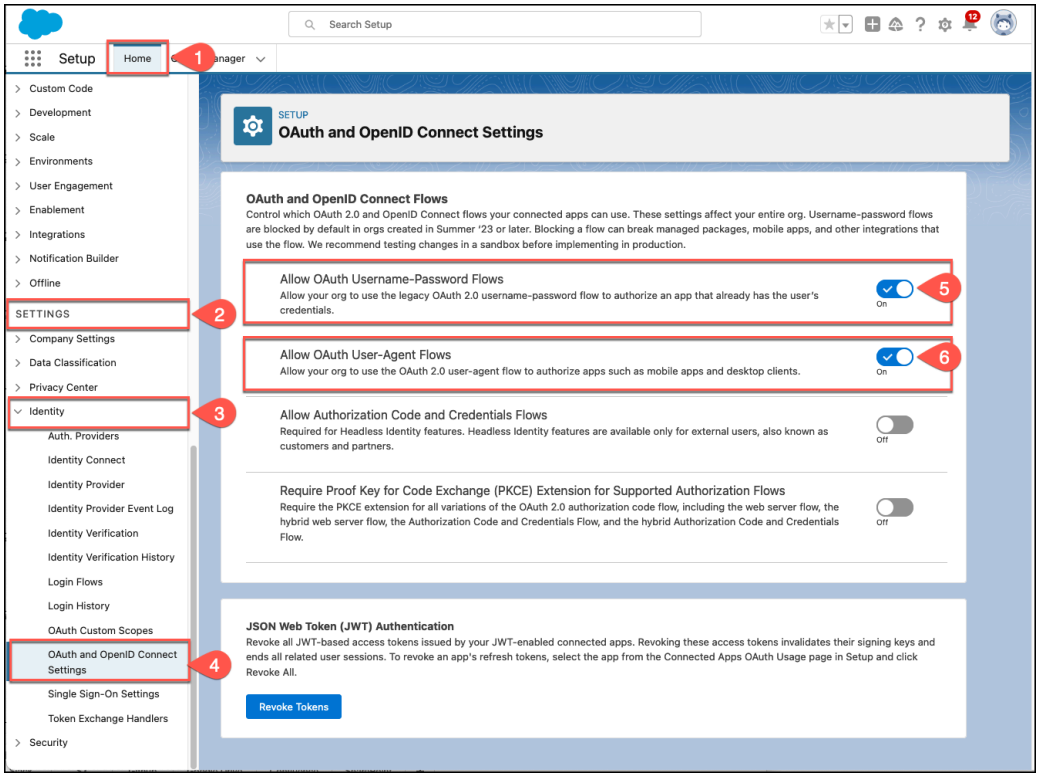


10. Then, from the left navigation menu, select **My Personal Information**. Then, select **Reset My Security Token**. Your security token will be sent to the email address connect to your Salesforce Online instance. You need this security token to connect Salesforce Online to Amazon Q.



11. Then, you activate OAuth Username-Password Flow for the Salesforce Online Connected App you've created. From the left navigation menu, from **Settings**, select **Identity** and then select **OAuth and OpenID Connect Settings**.

12. On the **OAuth and OpenID Connect Settings**, in **OAuth and OpenID Connect Flows**, make sure that both **Allow OAuth Username-Password Flows** and **Allow OAuth User-Agent Flows** are activated.



You now have the Salesforce Online host URL, username, password, security token, client ID, client secret, and authentication URL you need to connect Salesforce Online to Amazon Q.

Connecting Amazon Q Business to Salesforce Online using the console

The following procedure outlines how to connect Amazon Q Business to Salesforce Online using the AWS Management Console.

Connecting Amazon Q to Salesforce Online

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Salesforce Online** data source to your Amazon Q application.
5. Then, on the **Salesforce Online** data source page, enter the following information:

6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. In **Source**, enter the following information:

   - **Salesforce URL** – Enter your Salesforce server URL. For example, *`https://mysite.salesforce.com`*.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. For **Username**, **Password**, **Security token**, **Consumer key**, **Consumer secret**, and **Authentication URL** – Enter the authentication credential values that you created in your Salesforce account.

      > **Note**
      >
      > If you use Salesforce Online Developer Edition, use `https://login.salesforce.com/services/oauth2/token` or the My Domain login URL (for example, *`https://MyCompany.my.salesforce.com`*) as the **Authentication URL**. If you use Salesforce Online Sandbox Edition, use `https://test.salesforce.com/services/oauth2/token` or the My Domain login URL (for example, *`MyDomainName--SandboxName.sandbox.my.salesforce.com`*) as the **Authentication URL**.

   c. Choose **Save and add secret**.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.

12. **Sync scope** – Set the content that you want to sync.

    a. For **Standard objects**, **Standard objects with attachments**, **Standard objects without attachments**, and **Knowledge articles** – Select Salesforce entities or content types you want to crawl.

    > **Note**
    >
    > You must provide configuration information for indexing at least one of standard objects, knowledge articles, or chatter feeds. If you choose to crawl **Knowledge articles** you must specify the types of knowledge articles to index, the name of the articles, and whether to index the standard fields of all knowledge articles or only the fields of a custom article type. If you choose to index custom articles, you must specify the internal name of the article type. You can specify up to 10 article types.

    b. For **Custom objects** – Add custom object names. You can choose to include custom object attachments as well.

c. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

To extract audio transcriptions and video content, enable processing for the following file types:

d. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

13. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
14. In **Additional configuration – *optional***:

- For **Entity regex patterns** and **Attachment regex patterns** – Add regular expression patterns to include or exclude certain files. You can add up to 100 patterns.

15. In **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

- **Full sync** – Sync all content regardless of the previous sync status.
- **New or modified content sync** – Sync only new and modified documents.
- **New, modified, or deleted content sync** – Sync only new, modified, and deleted documents.

For more details, see Sync mode.

16. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
17. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
18. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

19. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Salesforce using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Salesforce JSON schema

The following is the Salesforce JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties":
  {
    "connectionConfiguration": {
      "type": "object",
      "properties":
      {
        "repositoryEndpointMetadata":
        {
          "type": "object",
          "properties":
          {
            "hostUrl":
            {
              "type": "string",
              "pattern": "^https:\/\/[a-zA-Z0-9-./]*\\.(salesforce|force).com\/?$"
            }
          },
          "required":
          [
            "hostUrl"
          ]
        }
      },
      "required":
      [
        "repositoryEndpointMetadata"
```

```
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties":
      {
        "account":
        {
          "type": "object",
          "properties":
          {
            "fieldMappings":
            {
              "type": "array",
              "items":
              [
                {
                  "type": "object",
                  "properties":
                  {
                    "indexFieldName":
                    {
                      "type": "string"
                    },
                    "indexFieldType":
                    {
                      "type": "string",
                      "enum":
                      [
                        "STRING",
                        "STRING_LIST",
                        "DATE",
                        "LONG"
                      ]
                    },
                    "dataSourceFieldName":
                    {
                      "type": "string"
                    },
                    "dateFieldFormat":
                    {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
```

```
                },
                "required":
                [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required":
        [
          "fieldMappings"
        ]
      },
      "contact":
      {
        "type": "object",
        "properties":
        {
          "fieldMappings":
          {
            "type": "array",
            "items":
            [
              {
                "type": "object",
                "properties":
                {
                  "indexFieldName":
                  {
                    "type": "string"
                  },
                  "indexFieldType":
                  {
                    "type": "string",
                    "enum":
                    [
                      "STRING",
                      "STRING_LIST",
                      "DATE"
                    ]
                  },
```

```
                "dataSourceFieldName":
                {
                  "type": "string"
                },
                "dateFieldFormat":
                {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required":
              [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required":
      [
        "fieldMappings"
      ]
    },
    "campaign":
    {
      "type": "object",
      "properties":
      {
        "fieldMappings":
        {
          "type": "array",
          "items":
          [
            {
              "type": "object",
              "properties":
              {
                "indexFieldName":
                {
                  "type": "string"
                },
                "indexFieldType":
```

```
                {
                  "type": "string",
                  "enum":
                  [
                    "STRING",
                    "STRING_LIST",
                    "DATE",
                    "LONG"
                  ]
                },
                "dataSourceFieldName":
                {
                  "type": "string"
                },
                "dateFieldFormat":
                {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required":
              [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required":
      [
        "fieldMappings"
      ]
    },
    "case":
    {
      "type": "object",
      "properties":
      {
        "fieldMappings":
        {
          "type": "array",
          "items":
```

```
            [
              {
                "type": "object",
                "properties":
                {
                  "indexFieldName":
                  {
                    "type": "string"
                  },
                  "indexFieldType":
                  {
                    "type": "string",
                    "enum":
                    [
                      "STRING",
                      "STRING_LIST",
                      "DATE"
                    ]
                  },
                  "dataSourceFieldName":
                  {
                    "type": "string"
                  },
                  "dateFieldFormat":
                  {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required":
                [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required":
        [
          "fieldMappings"
        ]
      },
```

```
        "product":
        {
          "type": "object",
          "properties":
          {
            "fieldMappings":
            {
              "type": "array",
              "items":
              [
                {
                  "type": "object",
                  "properties":
                  {
                    "indexFieldName":
                    {
                      "type": "string"
                    },
                    "indexFieldType":
                    {
                      "type": "string",
                      "enum":
                      [
                        "STRING",
                        "STRING_LIST",
                        "DATE"
                      ]
                    },
                    "dataSourceFieldName":
                    {
                      "type": "string"
                    },
                    "dateFieldFormat":
                    {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required":
                  [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
```

```
            }
          ]
        }
      },
      "required":
      [
        "fieldMappings"
      ]
    },
    "lead":
    {
      "type": "object",
      "properties":
      {
        "fieldMappings":
        {
          "type": "array",
          "items":
          [
            {
              "type": "object",
              "properties":
              {
                "indexFieldName":
                {
                  "type": "string"
                },
                "indexFieldType":
                {
                  "type": "string",
                  "enum":
                  [
                    "STRING",
                    "STRING_LIST",
                    "DATE",
                    "LONG"
                  ]
                },
                "dataSourceFieldName":
                {
                  "type": "string"
                },
                "dateFieldFormat":
                {
```

```
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required":
                [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required":
        [
          "fieldMappings"
        ]
      },
      "contract":
      {
        "type": "object",
        "properties":
        {
          "fieldMappings":
          {
            "type": "array",
            "items":
            [
              {
                "type": "object",
                "properties":
                {
                  "indexFieldName":
                  {
                    "type": "string"
                  },
                  "indexFieldType":
                  {
                    "type": "string",
                    "enum":
                    [
                      "STRING",
                      "STRING_LIST",
```

```
                    "DATE"
                  ]
                },
                "dataSourceFieldName":
                {
                  "type": "string"
                },
                "dateFieldFormat":
                {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required":
              [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required":
      [
        "fieldMappings"
      ]
    },
    "partner":
    {
      "type": "object",
      "properties":
      {
        "fieldMappings":
        {
          "type": "array",
          "items":
          [
            {
              "type": "object",
              "properties":
              {
                "indexFieldName":
                {
```

```
                    "type": "string"
                  },
                  "indexFieldType":
                  {
                    "type": "string",
                    "enum":
                    [
                      "STRING",
                      "STRING_LIST",
                      "DATE"
                    ]
                  },
                  "dataSourceFieldName":
                  {
                    "type": "string"
                  },
                  "dateFieldFormat":
                  {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required":
                [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required":
        [
          "fieldMappings"
        ]
      },
      "profile":
      {
        "type": "object",
        "properties":
        {
          "fieldMappings":
          {
```

```
            "type": "array",
            "items":
            [
              {
                "type": "object",
                "properties":
                {
                  "indexFieldName":
                  {
                    "type": "string"
                  },
                  "indexFieldType":
                  {
                    "type": "string",
                    "enum":
                    [
                      "STRING",
                      "STRING_LIST",
                      "DATE"
                    ]
                  },
                  "dataSourceFieldName":
                  {
                    "type": "string"
                  },
                  "dateFieldFormat":
                  {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required":
                [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required":
        [
          "fieldMappings"
```

```
          ]
        },
        "idea":
        {
          "type": "object",
          "properties":
          {
            "fieldMappings":
            {
              "type": "array",
              "items":
              [
                {
                  "type": "object",
                  "properties":
                  {
                    "indexFieldName":
                    {
                      "type": "string"
                    },
                    "indexFieldType":
                    {
                      "type": "string",
                      "enum":
                      [
                        "STRING",
                        "STRING_LIST",
                        "DATE",
                        "LONG"
                      ]
                    },
                    "dataSourceFieldName":
                    {
                      "type": "string"
                    },
                    "dateFieldFormat":
                    {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required":
                  [
                    "indexFieldName",
```

```
                    "indexFieldType",
                    "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required":
        [
          "fieldMappings"
        ]
      },
      "pricebook":
      {
        "type": "object",
        "properties":
        {
          "fieldMappings":
          {
            "type": "array",
            "items":
            [
              {
                "type": "object",
                "properties":
                {
                  "indexFieldName":
                  {
                    "type": "string"
                  },
                  "indexFieldType":
                  {
                    "type": "string",
                    "enum":
                    [
                      "STRING",
                      "STRING_LIST",
                      "DATE"
                    ]
                  },
                  "dataSourceFieldName":
                  {
                    "type": "string"
                  },
```

```
                  "dateFieldFormat":
                  {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required":
                [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required":
        [
          "fieldMappings"
        ]
      },
      "task":
      {
        "type": "object",
        "properties":
        {
          "fieldMappings":
          {
            "type": "array",
            "items":
            [
              {
                "type": "object",
                "properties":
                {
                  "indexFieldName":
                  {
                    "type": "string"
                  },
                  "indexFieldType":
                  {
                    "type": "string",
                    "enum":
                    [
```

```
                    "STRING",
                    "STRING_LIST",
                    "DATE"
                  ]
                },
                "dataSourceFieldName":
                {
                  "type": "string"
                },
                "dateFieldFormat":
                {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required":
              [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required":
      [
        "fieldMappings"
      ]
    },
    "solution":
    {
      "type": "object",
      "properties":
      {
        "fieldMappings":
        {
          "type": "array",
          "items":
          [
            {
              "type": "object",
              "properties":
              {
```

```
                  "indexFieldName":
                  {
                    "type": "string"
                  },
                  "indexFieldType":
                  {
                    "type": "string",
                    "enum":
                    [
                      "STRING",
                      "STRING_LIST",
                      "DATE"
                    ]
                  },
                  "dataSourceFieldName":
                  {
                    "type": "string"
                  },
                  "dateFieldFormat":
                  {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required":
                [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required":
        [
          "fieldMappings"
        ]
      },
      "attachment":
      {
        "type": "object",
        "properties":
        {
```

```
            "fieldMappings":
            {
              "type": "array",
              "items":
              [
                {
                  "type": "object",
                  "properties":
                  {
                    "indexFieldName":
                    {
                      "type": "string"
                    },
                    "indexFieldType":
                    {
                      "type": "string",
                      "enum":
                      [
                        "STRING",
                        "STRING_LIST",
                        "DATE",
                        "LONG"
                      ]
                    },
                    "dataSourceFieldName":
                    {
                      "type": "string"
                    },
                    "dateFieldFormat":
                    {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required":
                  [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
```

```
          "required":
          [
            "fieldMappings"
          ]
        },
        "user":
        {
          "type": "object",
          "properties":
          {
            "fieldMappings":
            {
              "type": "array",
              "items":
              [
                {
                  "type": "object",
                  "properties":
                  {
                    "indexFieldName":
                    {
                      "type": "string"
                    },
                    "indexFieldType":
                    {
                      "type": "string",
                      "enum":
                      [
                        "STRING",
                        "STRING_LIST",
                        "DATE"
                      ]
                    },
                    "dataSourceFieldName":
                    {
                      "type": "string"
                    },
                    "dateFieldFormat":
                    {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required":
```

```
                [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required":
        [
          "fieldMappings"
        ]
      },
      "document":
      {
        "type": "object",
        "properties":
        {
          "fieldMappings":
          {
            "type": "array",
            "items":
            [
              {
                "type": "object",
                "properties":
                {
                  "indexFieldName":
                  {
                    "type": "string"
                  },
                  "indexFieldType":
                  {
                    "type": "string",
                    "enum":
                    [
                      "STRING",
                      "STRING_LIST",
                      "DATE",
                      "LONG"
                    ]
                  },
                  "dataSourceFieldName":
```

```
                {
                  "type": "string"
                },
                "dateFieldFormat":
                {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required":
              [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required":
      [
        "fieldMappings"
      ]
    },
    "knowledgeArticles":
    {
      "type": "object",
      "properties":
      {
        "fieldMappings":
        {
          "type": "array",
          "items":
          [
            {
              "type": "object",
              "properties":
              {
                "indexFieldName":
                {
                  "type": "string"
                },
                "indexFieldType":
                {
```

```
                    "type": "string",
                    "enum":
                    [
                      "STRING",
                      "STRING_LIST",
                      "DATE"
                    ]
                  },
                  "dataSourceFieldName":
                  {
                    "type": "string"
                  },
                  "dateFieldFormat":
                  {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required":
                [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required":
        [
          "fieldMappings"
        ]
      },
      "group":
      {
        "type": "object",
        "properties":
        {
          "fieldMappings":
          {
            "type": "array",
            "items":
            [
              {
```

```
                "type": "object",
                "properties":
                {
                  "indexFieldName":
                  {
                    "type": "string"
                  },
                  "indexFieldType":
                  {
                    "type": "string",
                    "enum":
                    [
                      "STRING",
                      "STRING_LIST",
                      "DATE"
                    ]
                  },
                  "dataSourceFieldName":
                  {
                    "type": "string"
                  },
                  "dateFieldFormat":
                  {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required":
                [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required":
        [
          "fieldMappings"
        ]
      },
      "opportunity":
      {
```

```
          "type": "object",
          "properties":
          {
            "fieldMappings":
            {
              "type": "array",
              "items":
              [
                {
                  "type": "object",
                  "properties":
                  {
                    "indexFieldName":
                    {
                      "type": "string"
                    },
                    "indexFieldType":
                    {
                      "type": "string",
                      "enum":
                      [
                        "STRING",
                        "STRING_LIST",
                        "DATE",
                        "LONG"
                      ]
                    },
                    "dataSourceFieldName":
                    {
                      "type": "string"
                    },
                    "dateFieldFormat":
                    {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required":
                  [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
```

```
            ]
          }
        },
        "required":
        [
          "fieldMappings"
        ]
      },
      "chatter":
      {
        "type": "object",
        "properties":
        {
          "fieldMappings":
          {
            "type": "array",
            "items":
            [
              {
                "type": "object",
                "properties":
                {
                  "indexFieldName":
                  {
                    "type": "string"
                  },
                  "indexFieldType":
                  {
                    "type": "string",
                    "enum":
                    [
                      "STRING",
                      "STRING_LIST",
                      "DATE"
                    ]
                  },
                  "dataSourceFieldName":
                  {
                    "type": "string"
                  },
                  "dateFieldFormat":
                  {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
```

```
                    }
                  },
                  "required":
                  [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required":
          [
            "fieldMappings"
          ]
        },
        "customEntity":
        {
          "type": "object",
          "properties":
          {
            "fieldMappings":
            {
              "type": "array",
              "items":
              [
                {
                  "type": "object",
                  "properties":
                  {
                    "indexFieldName":
                    {
                      "type": "string"
                    },
                    "indexFieldType":
                    {
                      "type": "string",
                      "enum":
                      [
                        "STRING",
                        "STRING_LIST",
                        "DATE"
                      ]
```

```
                    },
                    "dataSourceFieldName":
                    {
                      "type": "string"
                    },
                    "dateFieldFormat":
                    {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required":
                  [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required":
          [
            "fieldMappings"
          ]
        }
      }
    },
    "additionalProperties": {
      "type": "object",
      "properties":
      {
        "accountFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "contactFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
```

```
          }
        },
        "caseFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "campaignFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "contractFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "groupFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "leadFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "productFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
```

```
        "opportunityFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "partnerFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "pricebookFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "ideaFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "profileFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "taskFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "solutionFilter":{
          "type": "array",
```

```
          "items":
          {
            "type": "string"
          }
        },
        "userFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "chatterFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "documentFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "knowledgeArticleFilter":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "customEntities":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "isCrawlAcl": {
          "type": "boolean"
        },
        "maxFileSizeInMegaBytes": {
```

```
          "type": "string"
        },
        "fieldForUserId": {
          "type": "string"
        },
        "isCrawlAccount": {
          "type": "boolean"
        },
        "isCrawlContact": {
          "type": "boolean"
        },
        "isCrawlCase": {
          "type": "boolean"
        },
        "isCrawlCampaign": {
          "type": "boolean"
        },
        "isCrawlProduct": {
          "type": "boolean"
        },
        "isCrawlLead": {
          "type": "boolean"
        },
        "isCrawlContract": {
          "type": "boolean"
        },
        "isCrawlPartner": {
          "type": "boolean"
        },
        "isCrawlProfile": {
          "type": "boolean"
        },
        "isCrawlIdea": {
          "type": "boolean"
        },
        "isCrawlPricebook": {
          "type": "boolean"
        },
        "isCrawlDocument": {
          "type": "boolean"
        },
        "crawlSharedDocument": {
          "type": "boolean"
        },
```

```
        "isCrawlGroup": {
          "type": "boolean"
        },
        "isCrawlOpportunity": {
          "type": "boolean"
        },
        "isCrawlChatter": {
          "type": "boolean"
        },
        "isCrawlUser": {
          "type": "boolean"
        },
        "isCrawlSolution":{
          "type": "boolean"
        },
        "isCrawlTask":{
          "type": "boolean"
        },

        "isCrawlAccountAttachments": {
          "type": "boolean"
        },
        "isCrawlContactAttachments": {
          "type": "boolean"
        },
        "isCrawlCaseAttachments": {
          "type": "boolean"
        },
        "isCrawlCampaignAttachments": {
          "type": "boolean"
        },
        "isCrawlLeadAttachments": {
          "type": "boolean"
        },
        "isCrawlContractAttachments": {
          "type": "boolean"
        },
        "isCrawlGroupAttachments": {
          "type": "boolean"
        },
        "isCrawlOpportunityAttachments": {
          "type": "boolean"
        },
        "isCrawlChatterAttachments": {
```

```
          "type": "boolean"
        },
        "isCrawlSolutionAttachments":{
          "type": "boolean"
        },
        "isCrawlTaskAttachments":{
          "type": "boolean"
        },
        "isCrawlCustomEntityAttachments":{
          "type": "boolean"
        },
        "isCrawlKnowledgeArticles": {
          "type": "object",
          "properties":
          {
            "isCrawlDraft": {
              "type": "boolean"
            },
            "isCrawlPublish": {
              "type": "boolean"
            },
            "isCrawlArchived": {
              "type": "boolean"
            }
          }
        },
        "inclusionDocumentFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionDocumentFileTypePatterns": {
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionDocumentFileNamePatterns":{
          "type": "array",
          "items":
          {
```

```
            "type": "string"
          }
        },
        "exclusionDocumentFileNamePatterns": {
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionAccountFileTypePatterns": {
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionAccountFileTypePatterns": {
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionAccountFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionAccountFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionCampaignFileTypePatterns": {
          "type": "array",
          "items":
          {
            "type": "string"
          }
```

```
        },
        "exclusionCampaignFileTypePatterns": {
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionCampaignFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionCampaignFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionCaseFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionCaseFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionCaseFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionCaseFileNamePatterns":{
```

```
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionContactFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionContactFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionContactFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionContactFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionContractFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionContractFileTypePatterns":{
          "type": "array",
          "items":
```

```
          {
            "type": "string"
          }
        },
        "inclusionContractFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionContractFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionLeadFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionLeadFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionLeadFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionLeadFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
```

```
        }
      },
      "inclusionOpportunityFileTypePatterns":{
        "type": "array",
        "items":
        {
          "type": "string"
        }
      },
      "exclusionOpportunityFileTypePatterns":{
        "type": "array",
        "items":
        {
          "type": "string"
        }
      },
      "inclusionOpportunityFileNamePatterns":{
        "type": "array",
        "items":
        {
          "type": "string"
        }
      },
      "exclusionOpportunityFileNamePatterns":{
        "type": "array",
        "items":
        {
          "type": "string"
        }
      },
      "inclusionSolutionFileTypePatterns":{
        "type": "array",
        "items":
        {
          "type": "string"
        }
      },
      "exclusionSolutionFileTypePatterns":{
        "type": "array",
        "items":
        {
          "type": "string"
        }
      },
```

```
        "inclusionSolutionFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionSolutionFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionTaskFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionTaskFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionTaskFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionTaskFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionGroupFileTypePatterns":{
          "type": "array",
```

```
          "items":
          {
            "type": "string"
          }
        },
        "exclusionGroupFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionGroupFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionGroupFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionChatterFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionChatterFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionChatterFileNamePatterns":{
          "type": "array",
          "items":
          {
```

```
            "type": "string"
          }
        },
        "exclusionChatterFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionCustomEntityFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionCustomEntityFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "inclusionCustomEntityFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionCustomEntityFileNamePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        }
      },
      "required":
      []
    },
    "enableIdentityCrawler": {
      "type": "boolean"
```

```
    },
    "type": {
      "type": "string",
   "enum": [
     "SALESFORCEV2",
     "SALESFORCE"
   ]
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FULL_CRAWL",
        "FORCED_FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the endpoint for the data source.
`repositoryEndpointMetadata`	The endpoint information for the data source.
`hostUrl`	The URL of the Salesforce instance to be indexed.
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.
• `account` • `contact` • `campaign` • `case` • `product` • `lead` • `contract` • `partner` • `profile` • `idea` • `pricebook` • `task` • `solution` • `attachment` • `user` • `document` • `knowledgeArticles` • `group` • `opportunity`	A list of objects that map the attributes or field names of your Salesforce entities to Amazon Q index field names.

Configuration	Description
• chatter • customEntity	
additionalProperties	Additional configuration options for your content in your data source.
• accountFilter • contactFilter • caseFilter • campaignFilter • contractFilter • groupFilter • leadFilter • productFilter • opportunityFilter • partnerFilter • pricebookFilter • ideaFilter • profileFilter • taskFilter • solutionFilter • userFilter • chatterFilter • documentFilter • knowledgeArticleFilter	Filters to specify content for Amazon Q to crawl.
customEntities	Custom entities that Amazon Q should crawl.

Configuration	Description
`inclusionPatterns` • `inclusionDocumentFileTypePatterns` • `inclusionDocumentFileNamePatterns` • `inclusionAccountFileTypePatterns` • `inclusionCampaignFileTypePatterns` • `inclusionDocumentFileNamePatterns` • `inclusionCampaignFileNamePatterns` • `inclusionCaseFileTypePatterns` • `inclusionCaseFileNamePatterns` • `inclusionContactFileTypePatterns` • `inclusionContractFileNamePatterns` • `inclusionLeadFileTypePatterns` • `inclusionLeadFileNamePatterns` • `inclusionOpportunityFileTypePatterns` • `inclusionOpportunityFileNamePatterns` • `inclusionSolutionFileTypePatterns` • `inclusionSolutionFileNamePatterns` • `inclusionTaskFileTypePatterns`	A list of regular expression patterns to *include* specific files in your Salesforce data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.

Configuration	Description
• inclusionTaskFileNamePatterns • inclusionGroupFileTypePatterns • inclusionGroupFileNamePatterns • inclusionChatterFileTypePatterns • inclusionChatterFileNamePatterns • inclusionCustomEntityFileTypePatterns • inclusionCustomEntityFileNamePatterns	

Configuration	Description
`exclusionPatterns` • `exclusionDocumentFileTypePatterns` • `exclusionDocumentFileNamePatterns` • `exclusionAccountFileTypePatterns` • `exclusionCampaignFileTypePatterns` • `exclusionCampaignFileNamePatterns` • `exclusionCaseFileTypePatterns` • `exclusionCaseFileNamePatterns` • `exclusionContactFileTypePatterns` • `exclusionContractFileNamePatterns` • `exclusionLeadFileTypePatterns` • `exclusionLeadFileNamePatterns` • `exclusionOpportunityFileTypePatterns` • `exclusionOpportunityFileNamePatterns` • `exclusionSolutionFileTypePatterns` • `exclusionSolutionFileNamePatterns` • `exclusionTaskFileTypePatterns` • `exclusionTaskFileNamePatterns` • `exclusionGroupFileTypePatterns`	A list of regular expression patterns to *exclude* specific files in your Salesforce data source. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an exclusion and inclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.

Configuration	Description
• exclusionGroupFileNamePatterns • exclusionChatterFileTypePatterns • exclusionChatterFileNamePatterns • exclusionCustomEntityFileTypePatterns • exclusionCustomEntityFileNamePatterns	
isCrawlAcl	Specify true to crawl access control information from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.
maxFileSizeInMegaBytes	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
fieldForUserId	Specify field to use for UserId for ACL crawling.

Configuration	Description
• isCrawlAccount • isCrawlContact • isCrawlCase • isCrawlCampaign • isCrawlProduct • isCrawlLead • isCrawlContract • isCrawlPartner • isCrawlProfile • isCrawlIdea • isCrawlPricebook • isCrawlDocument • crawlSharedDocument • isCrawlGroup • isCrawlOpportunity • isCrawlChatter • isCrawlUser • isCrawlSolution • isCrawlTask • isCrawlAccountAttachments • isCrawlContactAttachments • isCrawlCaseAttachments • isCrawlCampaignAttachments • isCrawlLeadAttachments • isCrawlContractAttachments • isCrawlGroupAttachments • isCrawlOpportunityAttachments • isCrawlChatterAttachments	true to index corresponding files in your Salesforce account.

Configuration	Description

• isCrawlSolutionAttachments
• isCrawlTaskAttachments
• isCrawlCustomEntityAttachments
• isCrawlKnowledgeArticles
  • isCrawlDraft
  • isCrawlPublish
  • isCrawlArchived	

type	The type of data source. Specify SALESFORCE as your data source type.
enableIdentityCrawler	true to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to certain documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.

Configuration	Description
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index

Configuration	Description

secretARN	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Salesforce data source. The secret must contain a JSON structure with the following keys:
	
	{
	"authenticationUrl": "The OAUTH endpoint that Amazon Q connects to get an OAUTH token.",
	"consumerKey": "The application public key generated when you created your Salesforce application." ,
	"consumerSecret": "The application private key generated when you created your Salesforce application." ,
	"password": "The password associated with the user logging in to the Salesforce instance." ,
	"securityToken": "The token associated with the user account logging in to the Salesforce instance." ,
	"username": "The user name of the user logging in to the Salesforce instance."
	}

version	The version of this template that's currently supported.

How Amazon Q Business connector crawls Salesforce ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an Salesforce data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your Salesforce instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

You can apply ACL based chat filtering using Salesforce standard objects and chatter feeds. ACL based chat filtering isn't available for Salesforce knowledge articles.

For standard objects, the `_user_id` and `_group_ids` are used as follows:

- `_user_id` – The username of the Salesforce user.
- `_group_ids` – The group names in Salesforce.
  - Name of the Salesforce `Profile`
  - Name of the Salesforce `Group`
  - Name of the Salesforce `UserRole`
  - Name of the Salesforce `PermissionSet`

For chatter feeds, the `_user_id` and `_group_ids` are used as follows:

- `_user_id` – The username of the Salesforce user. Only available if the item is posted in the user's feed.
- `_group_ids` – Group IDs are used as follows. Only available if the feed item is posted in a chatter or collaboration group.
  - The name of the chatter or collaboration group.
  - If the group is public, `PUBLIC:ALL`.

Important

To maintain secure access control for Amazon Q Business, each user must have a unique email address across all connected data sources.
In Salesforce users can share an email address while having a different application-specific unique identifier. However, in Amazon Q Business email addresses act as unique identifiers. This means that if a document is shared with a particular user (for example, arnav_desai@example.com who is part of pentesters@example.com) on the basis of an

application-specific unique ID, every other user who shares pentesters@example.com (for example, xiulan_wang@example.com and efua_owusu@example.com, both of whom are part of pentesters@example.com) can receive Amazon Q Business responses with content from a document that was shared only with Arnav. Similarly, content created by Arnav that only he should be able to access via Amazon Q Business chat responses, could also be part of Amazon Q Business chat responses for Xiulan and Efua, because they share the same email address.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Salesforce Online data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

Important

Filtering using document attributes in chat is only supported through the API.

The Amazon Q Salesforce connector supports the following entities and the associated reserved and custom attributes.

Note

You can map any Salesforce field to the document title or document body Amazon Q reserved/default index fields.

Supported entities and field mappings

- Account
- Campaign
- Case
- Contact
- Contract
- Document
- Group
- Idea
- Lead
- Opportunity
- Partner
- Pricebook
- Product
- Solution
- Profile
- Task
- User
- Chatter

- Knowledge articles
- Attachments
- Custom object

Account

Amazon Q supports crawling Salesforce Online Accounts and offers the following account field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
authors	_authors	Default	String list
lastModifiedBy	sf_last_modified_by	Custom	String
shippingCity	sf_shipping_city	Custom	String
shippingCountry	sf_shipping_country	Custom	String
shippingState	sf_shipping_state	Custom	String
website	sf_website	Custom	String
industry	sf_industry	Custom	String
accountSource	sf_account_source	Custom	String
billingCity	sf_billing_city	Custom	String
billingCountry	sf_billing_country	Custom	String

Salesforce field name	Index field name	Description	Data type
billingState	sf_billing_state	Custom	String
createdBy	sf_created_by	Custom	String
lastActivityDate	sf_last_activity_date	Custom	Date
parentId	sf_parent_id	Custom	String
typeValue	sf_type_value	Custom	String
billingStreet	sf_billing_street	Custom	String
billingPostalCode	sf_billing_postal_code	Custom	String
billingLatitude	sf_billing_latitude	Custom	String
billingLongitude	sf_billing_longitude	Custom	String
billingGeocodeAccuracy	sf_billing_geocode_accuracy	Custom	String
shippingStreet	sf_shipping_street	Custom	String
shippingPostalCode	sf_shipping_postal_code	Custom	String
phone	sf_phone	Custom	String
fax	sf_fax	Custom	String
annualRevenue	sf_annual_revenue	Custom	String
numberOfEmployees	sf_number_of_employees	Custom	Long (numeric)
jigsaw	sf_jigsaw	Custom	String

Campaign

Amazon Q supports crawling Salesforce Online Campaigns and offers the following campaign field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
isActive	sf_is_active	Custom	String
updatedAt	_last_updated_at	Default	Date
ownerName	_authors	Default	String list
lastModifiedBy	sf_last_modified_by	Custom	String
createdBy	sf_created_by	Custom	String
lastActivityDate	sf_last_activity_date	Custom	Date
parentId	sf_parent_id	Custom	String
campaignName	sf_campaign_name	Custom	String
status	sf_status	Custom	String
parentName	sf_parent_name	Custom	String
campaignType	sf_type	Custom	String
expectedRevenue	sf_expected_revenue	Custom	Long (numeric)
budgetedCost	sf_budgeted_cost	Custom	Long (numeric)
actualCost	sf_actual_cost	Custom	Long(numeric)

Salesforce field name	Index field name	Description	Data type
expectedResponse	sf_expected_response	Custom	String
numberSent	sf_number_sent	Default	Long numeric)
numberOfLeads	sf_number_of_leads	Custom	Long (numeric)
numberOfConvertedLeads	sf_number_of_converted_leads	Custom	Long (numeric)
numberOfContacts	sf_number_of_contacts	Custom	Long (numeric)
numberOfResponses	sf_number_of_responses	Custom	Long (numeric)
numberOfOpportunites	sf_number_of_opportunities	Custom	Long (numeric)
numberOfWonOpportunities	sf_number_of_won_opportunitues	Custom	Long (numeric)
amountAllOpportunities	sf_amount_all_opportunities	Custom	Long (numeric)
amountWonOpportunities	sf_amount_won_opportunities	Custom	Long (numeric)

Case

Amazon Q supports crawling Salesforce Online Cases and offers the following case field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String

Salesforce field name	Index field name	Description	Data type
sourceUrl	_source_uri	Default	String
authors	_authors	Default	String list
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
ownerName	sf_owner_name	Custom	String
createdBy	sf_created_by	Custom	String
caseNumber	sf_case_number	Custom	String
isClosed	sf_is_closed	Custom	String
isEscalated	sf_is_escalated	Custom	String
priority	sf_priority	Custom	String
status	sf_status	Custom	String
accountName	sf_account_name	Custom	String
lastModifiedBy	af_last_modified_by	Custom	String
updatedAt	_last_updated_at	Default	Date
typeValue	sf_type	Custom	String
reason	sf_reason	Custom	String
contactId	sf_contact_id	Custom	String
origin	sf_origin	Custom	String
parentId	sf_parent_id	Custom	String
contactName	sf_contact_name	Custom	String

Salesforce field name	Index field name	Description	Data type
parentCaseNumber	sf_parent_case_number	Custom	String
parentSubject	sf_parent_subject	Custom	String
suppliedEmail	sf_supplied_email	Custom	String
contactPhone	sf_contact_phone	Custom	String
contactMobile	sf_contact_mobile	Custom	String
contactEmail	sf_contact_email	Custom	String
contactFax	sf_contact_fax	Custom	String
comments	sf_comments	Custom	String
lastViewedDate	sf_last_viewed_date	Custom	String

Contact

Amazon Q supports crawling Salesforce Online Contacts and offers the following contact field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
authors	_authors	Default	String list
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date

Salesforce field name	Index field name	Description	Data type
lastModifiedBy	sf_last_modified_by	Custom	String
lastActivityDate	sf_last_activity_date	Custom	Date
createdBy	sf_created_by	Custom	String
contactName	sf_contact_name	Custom	String
phone	sf_phone	Custom	String
email	sf_email	Custom	String
department	sf_department	Custom	String
lastname	sf_lastname	Custom	String
title	sf_title	Custom	String
reportsTo	sf_reports_to	Custom	String
account	sf_account	Custom	String
otherStreet	sf_other_street	Custom	String
otherCity	sf_other_city	Custom	String
otherState	sf_other_state	Custom	String
otherPostalCode	sf_other_postal_code	Custom	String
otherCountry	sf_other_country	Custom	String
otherLatitude	sf_other_latitude	Custom	String
otherLongitude	sf_other_longitude	Custom	String
otherGeocodeAccuracy	sf_other_geocode_accuracy	Custom	String

Salesforce field name	Index field name	Description	Data type
mailingStreet	sf_mailing_street	Custom	String
mailingCity	sf_mailing_city	Custom	String
mailingState	sf_mailing_state	Custom	String
mailingPostalCode	sf_mailing_postal_code	Custom	String
mailingCountry	sf_mailing_country	Custom	String
mailingLatitude	sf_mailing_latitude	Custom	String
mailingLongitude	sf_mailing_longitude	Custom	String
mailingGeocodeAccuracy	sf_mailing_geocode_accuracy	Custom	String
fax	sf_fax	Custom	String
mobilePhone	sf_mobile_phone	Custom	String
homePhone	sf_home_phone	Custom	String
otherPhone	sf_other_phone	Custom	String
assistantPhone	sf_assistant_phone	Custom	String
assistantName	sf_assistant_name	Custom	String
leadSource	sf_lead_source	Custom	String
birthDate	sf_birthdate	Custom	Date
jigsaw	sf_jigsaw	Custom	String

Contract

Amazon Q supports crawling Salesforce Online Contracts and offers the following contract field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
authors	_authors	Default	String list
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
authors	_authors	Default	String list
accountId	_sf_accoung_id	Custom	String
ownerExpirationNotice	sf_owner_expiration_notice	Custom	String
billingStreet	sf_billing_street	Custom	String
billingCity	sf_billing_city	Custom	String
billingState	sf_billing_state	Custom	String
billingPostalCode	sf_billing_postal_code	Custom	String
billingCountry	sf_billing_country	Custom	String
contractTerm	sf_contract_term	Custom	String
ownerId	sf_owner_id	Custom	String
status	sf_status	Custom	String

Salesforce field name	Index field name	Description	Data type
customerSignedTitle	sf_customer_signed_title	Custom	String
specialTerms	sf_special_terms	Custom	String
statusCode	sf_status_code	Custom	String
contractNumber	sf_contract_number	Custom	String
lastViewedDate	sf_last_viewed_date	Custom	Date
lastReferenceDate	sf_last_reference_date	Custom	Date
billingAddressCity	sf_billing_address_city	Custom	String
billingAddressCountry	sf_billing_address_country	Custom	String
billingAddressPostalCode	sf_billing_address_postal_code	Custom	String
billingAddressState	sf_billing_address_state	Custom	String
billingAddressStreet	sf_billing_address_street	Custom	String
pricebookDescription	sf_pricebook_description	Custom	String
pricebookId	sf_pricebook_id	Custom	String
billingLatitude	sf_billing_latitude	Custom	String
billingLongitude	sf_billing_longitude	Custom	String

Salesforce field name	Index field name	Description	Data type
billingGeocodeAccuracy	sf_billing_geocode_accuracy	Custom	String
companySignedId	sf_company_signed_id	Custom	String
companySignedDate	sf_company_signed_date	Custom	Date
customerSignedId	sf_customer_signed_id	Custom	String
activatedById	sf_activated_by_id	Custom	String
activatedDate	sf_activated_date	Custom	Date
lastApprovedDate	sf_last_approved_date	Custom	Date
lastActivityDate	sf_last_activity_date	Custom	Date
accountName	sf_account_name	Custom	String
startDate	sf_start_date	Custom	Date
endDate	sf_end_date	Custom	Date
createdBy	sf_created_by	Custom	String

Document

Amazon Q supports crawling Salesforce Online Documents and offers the following document field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
author	_authors	Default	String list
createdAt	_created_at	Default	Date
folder	sf_folder_name	Custom	String
isInternalUseOnly	sf_is_internal_use_only	Custom	String
isPublic	sf_is_public	Custom	String
keywords	sf_keywords	Custom	String
lastModifiedBy	sf_last_modified_by	Custom	String
updatedAt	_last_updated_at	Default	Date
fileName	sf_file_name	Custom	String
fileType	_file_type	Default	String
fileSize	sf_file_size	Custom	Long (numeric)
createdBy	sf_created_by	Custom	String
isBodySearchable	sf_is_body_searchable	Custom	String

Group

Amazon Q supports crawling Salesforce Online Groups and offers the following group field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
groupEmail	sf_group_email	Custom	String
lastModifiedBy	sf_last_modified_by	Custom	String
lastModifiedDate	_last_modified_at	Default	Date
ownerId	sf_owner_id	Custom	String
groupName	sf_group_name	Custom	String
createdBy	_authors	Default	String list
lastFeedModifiedDate	sf_last_feed_modified_date	Custom	Date
hasPrivateFieldsAccess	sf_has_private_fields_access	Custom	String
canHaveGuests	sf_can_have_guests	Custom	String
isArchived	sf_is_archived	Custom	String
isAutoArchived	sf_is_auto_archive_disabled	Custom	String
memberCount	sf_member_count	Custom	String
collaborationType	sf_collabotration_type	Custom	String
informationTitle	sf_information_title	Custom	String

Idea

Amazon Q supports crawling Salesforce Online Ideas and offers the following idea field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
lastModifiedBy	sf_last_modified_by	Custom	String
title	sf_title	Custom	String
status	sf_status	Custom	String
createdByName	sf_created_by	Custom	String
parentIdea	sf_parent_idea_id	Custom	String
parentIdeaId	sf_parent_idea_id	Custom	String
lastModifiedDate	_last_modified_at	Default	Date
recordTypeId	sf_record_type_id	Custom	String
communityId	sf_community_id	Custom	String
numComments	sf_number_of_comments	Custom	Long (numeric)
voteScore	sf_vote_score	Custom	Long (numeric)
voteTotal	sf_vote_total	Custom	Long (numeric)
lastCommentDate	sf_last_comment_date	Custom	Date

Lead

Amazon Q supports crawling Salesforce Online Leads and offers the following lead field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
city	sf_city	Custom	String
company	sf_company	Custom	String
country	sf_country	Custom	String
createdAt	_created_at	Default	Date
lastModifiedBy	sf_last_modified_by	Custom	String
updatedAt	_last_updated_at	Default	Date
leadSource	sf_lead_source	Custom	String
state	sf_state	Custom	String
status	sf_status	Custom	String
convertedAccount	sf_converted_account	Custom	String
convertedAccountId	sf_converted_account_id	Custom	String
convertedContact	sf_converted_contact	Custom	String
convertedContactId	sf_converted_contact_id	Custom	String
convertedDate	sf_converted_date	Custom	Date

Salesforce field name	Index field name	Description	Data type
convertedOpportunity	sf_converted_opportunity	Custom	String
convertedOpportunityId	sf_converted_opportunity_id	Custom	String
firstName	sf_first_name	Custom	String
createdBy	_authors	Default	String list
isConverted	sf_is_converted	Custom	String
owner	sf_owner_name	Custom	String
lastActivityDate	sf_last_activity_date	Custom	Date
ownerId	sf_owner_id	Custom	String
lastName	sf_last_name	Custom	String
title	sf_title	Custom	String
street	sf_street	Custom	String
postalCode	sf_postal_code	Custom	String
latitude	sf_latitude	Custom	String
longitude	sf_longitude	Custom	String
geocodeAccuracy	sf_geocode_accuracy	Custom	String
phone	sf_phone	Custom	String
email	sf_email	Custom	String
industry	sf_industry	Custom	String
rating	sf_rating	Custom	String

Salesforce field name	Index field name	Description	Data type
annualRevenue	sf_annual_revenue	Custom	String
numberofEmployees	sf_number_of_employees	Custom	Long (numeric)
jigsaw	sf_jigsaw	Custom	String
jigsawContactId	sf_jigsaw_contact_id	Custom	String
emailBouncedReason	sf_email_bounced_reason	Custom	String
individualId	sf_individual_id	Custom	String

Opportunity

Amazon Q supports crawling Salesforce Online Opportunities and offers the following opportunity field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
accountName	sf_account_name	Custom	String
amount	sf_amount	Custom	String
campaign	sf_campaign_name	Custom	String
createdAt	_created_at	Default	Date
createdBy	sf_created_by	Custom	String
lastModifiedBy	sf_last_modified_by	Custom	String

Salesforce field name	Index field name	Description	Data type
lastModifiedDate	_last_updated_at	Default	Date
fiscalQuarter	sf_fiscal_quarter	Custom	String
fiscalYear	sf_fiscal_year	Custom	String
isClosed	sf_is_closed	Custom	String
isWon	sf_is_won	Custom	String
leadSource	sf_lead_source	Custom	String
opportunityName	sf_opportunity_name	Custom	String
accountId	sf_account_id	Custom	String
campaignId	sf_campaign_id	Custom	String
closeDate	sf_close_date	Custom	Date
typeValue	sf_type_value	Custom	String
lastActivityDate	sf_last_activity_date	Date	String
ownerName	sf_owner_name	Custom	String
ownerId	sf_owner_id	Custom	String
stageName	sf_stage_name	Custom	String
probability	sf_probability	Custom	Long (numeric)
nextStep	sf_next_step	Custom	String
forestCategory	sf_forecast_category	Custom	String
forestCategoryName	sf_forest_category _name	Custom	String

Salesforce field name	Index field name	Description	Data type
hasOpportunityLineItem	sf_has_opportunity_line_item	Custom	String
pricebook2id	sf_pricebook2_id	Custom	String
pushCount	sf_push_count	Custom	String
fiscal	sf_fiscal	Custom	String
contactId	sf_contact_id	Custom	String
lastViewedDate	sf_last_viewed_date	Custom	Date
hasOpenActivity	sf_has_open_activity	Custom	Long (numeric)
hasOverdueTask	sf_has_overdue_task	Custom	String

Partner

Amazon Q supports crawling Salesforce Online Partner and offers the following partner field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
createdBy	_authors	Default	String list
opportunityId	sf_opportunity_id	Custom	String

Salesforce field name	Index field name	Description	Data type
accountFromId	sf_account_from_id	Custom	String
accountToId	sf_role	Custom	String
role	sf_role	Custom	String
isPrimary	sf_is_primary	Custom	String
systemModstamp	sf_system_modstamp	Custom	Date
reversePartnerId	sf_reverse_partner_id	Custom	String
opportunity	sf_opportunity	Custom	String
accountFrom	sf_account_from	Custom	String
accountTo	sf_account_to	Custom	String

Pricebook

Amazon Q supports crawling Salesforce Online Pricebooks and offers the following pricebook field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
isActive	sf_is_active	Custom	String
lastModifiedBy	sf_last_modified_by	Default	String
lastModifiedDate	_last_updated_at	Default	Date
pricebookName	sf_pricebook_name	Custom	String

Salesforce field name	Index field name	Description	Data type
createdAt	_created_at	Default	Date
createdBy	_authors	Default	String list
lastViewedDate	sf_last_viewed_date	Custom	Date
isStandard	sf_is_standard	Custom	String

Product

Amazon Q supports crawling Salesforce Online Product and offers the following product field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
family	sf_family	Custom	String
isActive	sf_is_active	Custom	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
lastModifiedBy	sf_last_modified_by	Custom	String
productCode	sf_product_code	Custom	String
createdBy	_authors	Default	String list
productName	sf_product_name	Custom	String

Salesforce field name	Index field name	Description	Data type
externalDataSourceId	sf_external_datasource_id	Custom	String
externalId	sf_external_id	Custom	String
displayUrl	sf_display_url	Custom	String
quantityUnitOfMeasure	sf_quantity_unit_of_measure	Custom	String
isArchived	sf_is_archived	Custom	String
lastViewedDate	sf_last_viewed_date	Custom	Date
stockKeepingUnit	sf_stock_keeping_unit	Custom	String

Solution

Amazon Q supports crawling Salesforce Online Solutions and offers the following solution field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
isPublished	sf_is_published	Custom	String
isReviewed	sf_is_reviewed	Custom	String
lastModifiedBy	sf_last_modified_by	Custom	String
lastModifiedDate	_last_updated_at	Default	Date

Salesforce field name	Index field name	Description	Data type
ownerName	sf_owner_name	Custom	String
solutionNumber	sf_solution_number	Custom	String
status	sf_status	Custom	String
timesUsed	sf_times_used	Custom	String
solutionName	sf_solution_name	Custom	String
createdByName	_authors	Default	String list
createdAt	_created_at	Default	Date
solutionNote	sf_solution_note	Custom	String
ownderId	sf_ownderId	Custom	String
lastViewedDate	sf_last_viewed_date	Custom	Date

Profile

Amazon Q supports crawling Salesforce Online Profiles and offers the following profile field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
updatedAt	_last_updated_at	Default	Date
lastModifiedBy	sf_last_modified_by	Custom	String
createdBy	_authors	Default	String list

Salesforce field name	Index field name	Description	Data type
createdAt	_created_at	Default	Date
userType	sf_user_type	Custom	String

Task

Amazon Q supports crawling Salesforce Online Tasks and offers the following task field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
accountName	sf_account_name	Custom	String
lastModifiedBy	sf_last_modified_by	Custom	String
lastModifiedDate	_last_updated_at	Default	Date
ownerName	sf_owner_name	Custom	String
isRecurrence	sf_is_recurrence	Custom	String
isClosed	sf_is_closed	Custom	String
isArchived	sf_is_archived	Custom	String
priority	sf_priority	Custom	String
status	sf_status	Custom	String
whatId	sf_what_id	Custom	String
createdByName	_authors	Default	String list

Salesforce field name	Index field name	Description	Data type
createdAt	_created_at	Default	Date
subject	sf_subject	Custom	String
activityDate	sf_activity_date	Custom	Date
activityDate	sf_activity_date	Custom	Date
isHighPriority	sf_is_high_priority	Custom	String
ownerId	sf_owner_id	Custom	String
callType	sf_call_type	Custom	String

User

Amazon Q supports crawling Salesforce Online Users and offers the following user field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
account	sf_account	Custom	String
isActive	sf_is_active	Custom	String
city	sf_city	Custom	String
lastModifiedBy	sf_last_modified_by	Custom	String
updatedAt	_last_updated_at	Default	Date
companyName	sf_company_name	Custom	String

Salesforce field name	Index field name	Description	Data type
country	sf_country	Custom	String
department	sf_department	Custom	String
division	sf_division	Custom	String
email	sf_email	Custom	String
employeeNumber	sf_employee_number	Custom	String
firstName	sf_first_name	Custom	String
lastName	sf_last_name	Custom	String
manager	sf_manager	Custom	String
state	sf_state	Custom	String
userRole	sf_user_role	Custom	String
username	sf_username	Custom	String
createdBy	_authors	Default	String list
createdAt	_created_at	Default	Date
street	sf_street	Custom	String
postalCode	sf_postal_code	Custom	String
latitude	sf_latitiude	Custom	String
longitude	sf_longitude	Custom	String
geocodeAccuracy	sf_geocode_accuracy	Custom	String
phone	sf_phone	Custom	String
fax	sf_fax	Custom	String

Salesforce field name	Index field name	Description	Data type
mobilePhone	sf_mobile_phone	Custom	String
profileName	sf_profile_name	Custom	String
aboutMe	sf_about_me	Custom	String
languageLocaleKey	sf_language_locale_key	Custom	String

Chatter

Amazon Q supports crawling Salesforce Online Chatters and offers the following chatter field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
body	sf_body	Custom	String
createdAt	_created_at	Default	Date
lastEditById	sf_last_edit_by_id	Custom	String
lastEditDate	sf_last_edit_date	Custom	Date
lastModifiedDate	_last_updated_at	Default	Date
insertedById	sf_inserted_by_id	Custom	String
createdBy	_authors	Default	String list
parentId	sf_parent_id	Custom	String

Salesforce field name	Index field name	Description	Data type
revision	sf_revision	Custom	String
status	sf_status	Custom	String
isRichText	sf_is_rich_texrt	Custom	String

Knowledge articles

Amazon Q supports crawling Salesforce Online Knowledge articles and offers the following knowledge article field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
articleTitle	sf_title	Custom	String
articleNumber	sf_article_number	Default	Date
knowledgeArticleId	sf_knowledge_article_id	Custom	String
lastPublishedDate	sf_last_published_date	Custom	Date
publishStatus	sf_publish_status	Custom	String
versionNumber	sf_version_number	Custom	String
language	sf_language	Custom	String
ownerId	sf_ownder_id	Custom	String
summary	sf_summary	Custom	String

Salesforce field name	Index field name	Description	Data type
firstPublishedDate	sf_first_published_date	Custom	Date
updatedAt	_last_updated_at	Default	Date
archivedDate	sf_archived_date	Custom	Date
isLatestVersion	sf_is_latest_version	Custom	String
sourceId	sf_sourceId	Custom	String
createdBy	_authors	Default	String list
assignmentDate	sf_assignment_date	Custom	Long (numeric)
assignmentDueDate	sf_assignment_due_date	Custom	Date
articleCaseAttachCount	sf_article_case_attach_count	Custom	Long (numeric)
articleTotalViewCount	sf_article_total_view_count	Custom	Long (numeric)
urlName	sf_url_name	Custom	String
assignmentNote	sf_assignment_date	Custom	String
migratedToFromArticleVersion	sf_migrated_article_version	Custom	String
assignedBy	sf_assigned_by	Custom	String
assignedTo	sf_assigned_to	Custom	Date

Attachments

Amazon Q supports crawling Salesforce Online Attachments and offers the following attachment field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
fileName	sf_file_name	Custom	String
fileType	_file_type	Default	String
fileSize	sf_file_size	Custom	Long (numeric)
parentName	sf_parent_name	Default	String
createdBy	_authors	Default	String list

Custom object

Amazon Q supports crawling custom objects and offers the following custom object field mappings.

Salesforce field name	Index field name	Description	Data type
category	_category	Default	String
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date

Salesforce field name	Index field name	Description	Data type
updatedAt	_last_updated_at	Default	Date
lastModifiedById	sf_last_modified_by_id	Custom	String
customObjectName	sf_custom_object_name	Custom	String
createdBy	_authors	Default	String list
lastModifiedBy	sf_last_modified_by	Custom	String
documentbody	_document_body	Custom	String

IAM role for Salesforce Online connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
```

```
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
```

```
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Troubleshooting your Salesforce Online connector

The following table provides information about error codes you may see for the Salesforce Online connector and suggested resolutions.

Error code	Error message	Suggested resolution
SF-5001	Invalid HostURL.	Provide valid HostURL.

Error code	Error message	Suggested resolution
SF-5002	Invalid userName or password.	Provide valid userName or password.
SF-5003	Invalid clientSecret.	Provide valid clientSecret.
SF-5004	Invalid clientId.	Provide valid clientId.
SF-5005	Invalid grant type.	Provide valid grant type.
SF-5006	Error while generating Access Token.	Provide valid credentials or try again later.
SF-5100	Null/empty HostUrl.	Provide HostUrl.
SF-5101	Null/empty client ID.	Provide client ID.
SF-5102	Null/empty client secret	Provide client secret.
SF-5103	Null/empty username.	Provide username.
SF-5104	Null/empty password.	Provide password.
SF-5150	Null/empty authentic ation URL.	Provide authentication URL.
SF-5151	Invalid HostURL pattern.	Provide valid HostURL pattern.
SF-5152	Invalid Authentication URL.	Provide valid Authentication URL.
SF-5500	ContinuableInterna lServerError.	Try again later.

Connecting ServiceNow Online to Amazon Q Business

ServiceNow provides a cloud-based service management system to create and manage organization-level workflows, such as IT services, ticketing systems, and support. You can connect

ServiceNow Online instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the Amazon Q Business ServiceNow Online connector
- ServiceNow Online connector overview
- Prerequisites for connecting Amazon Q Business to ServiceNow Online
- Connecting Amazon Q Business to ServiceNow Online using the console
- Connecting Amazon Q Business to ServiceNow using APIs
- Connecting Amazon Q Business to ServiceNow using AWS CloudFormation
- How Amazon Q Business connector crawls ServiceNow ACLs
- ServiceNow Online data source connector field mappings
- IAM role for Amazon Q Business ServiceNow Online connector
- Understand error codes in the Amazon Q Business ServiceNow Online connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Amazon Q Business ServiceNow Online connector

The ServiceNow Online connector has the following known limitations:

- There is no REST API to wake up your ServiceNow instance. To activate it when it's in hibernation mode, log in to the your ServiceNow instance.
- Because Amazon Q Business uses email address as unique identifiers, each user must have a unique email address.
- We don't support ServiceNow access controls.

- We don't support ServiceNow user criteria.
- Only the following ServiceNow roles are supported for incidents:
  - ITIL: This role provides broad access to incident management functionality.
  - Custom roles: You can create custom roles with specific incident access permissions.

ServiceNow Online connector overview

The following table gives an overview of the Amazon Q Business ServiceNow Online connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Basic, OAuth 2.0 with Resource Owner Password Flow
	Authentication credentials	**Basic** • ServiceNow Online host URL • User name • Password • ServiceNow Online version **OAuth 2.0 with Resource Owner Password Flow** • ServiceNow Online host URL • User name • Password • Client ID • Client secret • ServiceNow Online version

Category	Feature	Support
		Important ServiceNow Online admin privileges required.
	Supported versions	All ServiceNow versions
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	Yes. Supports custom fields for all entities.

Category	Feature	Support
	Entities	Yes. The following entities are supported: • Knowledge articles • Knowledge article attachments • Service catalogs • Active service catalog items • Inactive service catalog items • Service catalog attachments • Incidents • Active incidents • Inactive incidents • All active incident types • Resolved incidents • Open incidents • Open – Unassigned incidents • Incident attachments See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.

Category	Feature	Support
	Filters	Yes. The following filters are supported : • Crawl public knowledge articles • Crawl knowledge articles with filter query • Crawl knowledge article attachments • Use regex filters for knowledge articles • Crawl service catalog items • Crawl service catalog item attachments • Use regex filters for service catalog items • Crawl incidents • Crawl incident attachments • Crawl incidents with filter query • Use regex filters for active and inactive incidents • Including and excluding content by file type • Including and excluding content based on file name • Crawl ACL for knowledge article, service catalogs, and incidents
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.

Prerequisites for connecting Amazon Q Business to ServiceNow Online

Before you begin, make sure that you have completed the following prerequisites.

In ServiceNow, make sure you have:

- Created a Personal or Enterprise Developer Instance and have a ServiceNow instance with an administrative role.
- Copied the host of your ServiceNow instance URL. The format for the host URL you enter is *`your-domain.service-now.com`*. You need your ServiceNow instance URL to connect to Amazon Q.
- Configured basic authentication credentials containing a username and password to allow Amazon Q to connect to your ServiceNow instance.
- **Optional:** Configured an OAuth 2.0 credential token that can identify Amazon Q using a username, password, and a generated client ID, and a client secret. For more information, see ServiceNow documentation on OAuth 2.0 authentication on the ServiceNow website.
- Depending on what you are searching for, you will need specific roles. Note that if you are searching through public articles, you don't require any specific role. Apply the following roles depending on your use case:
  - When searching Knowledge article documents in Amazon Q, the user should have any of the following roles - Knowledge, Knowledge_Admin, and User_Admin or Itil.
  - When searching Service Catalog documents in Amazon Q, the user should have a catalog role.
  - When searching the Incident document in Amazon Q, the user should have the incident_manager role.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your ServiceNow Online authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

> **Note**
>
> For more information on connecting ServiceNow Online to Amazon Q Business, see Derive generative AI-powered insights from ServiceNow with Amazon Q Business in the *AWS Machine Learning Blog*.

Connecting Amazon Q Business to ServiceNow Online using the console

The following procedure outlines how to connect Amazon Q Business to ServiceNow Online using the AWS Management Console.

Connecting Amazon Q to ServiceNow Online

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **ServiceNow Online** data source to your Amazon Q application.
5. Then, on the **ServiceNow Online** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. In **Source**, enter the following information:

   - **ServiceNow host** – Enter your ServiceNow host name without the protocol. For example, *example.service-now.com*.

8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.

9. **Authentication** – Choose between **Basic authentication** and **OAuth 2.0 authentication** and then enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. Basic Authentication – Enter the **Secret name**, **Username**, and **Password** for your ServiceNow account.

      If using OAuth2 Authentication – Enter the **Secret name**, **Username**, **Password**, **Client ID**, and **Client Secret** that you created in your ServiceNow account.

   c. Choose **Save and add secret**.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

12. **Sync scope** – Set the content that you want to sync.

    a. For **Knowledge articles**, choose from the following options :

    - **Knowledge articles** – Choose to index knowledge articles.
    - **Knowledge article attachments** – Choose to index knowledge article attachments.
    - **Type of knowledge articles** – Choose between **Only public articles** and **Knowledge articles based on ServiceNow filter query**, based on your use case. If you select **Include articles based on ServiceNow filter query**, you must enter a **Filter query** copied from your ServiceNow account. Example filter queries include: *workflow_state=draft^EQ*, *kb_knowledge_base=dfc19531bf2021003f07e2c1ac0739ab^text ISNOTEMPTY^EQ*, and *article_type=text^active=true^EQ*.

      > **Important**
      >
      > If you choose to crawl **Only public articles**, Amazon Q crawls only knowledge articles assigned a public access role in ServiceNow Online.

    - **Include articles based on short description filter** – Specify regular expression patterns to include or exclude specific articles. For example, use `.*article[1,2].*` to include articles containing `article1` or `article2.` in their short descriptions. Use `(^mystart.*|.*endwith$)` to crawl articles with short descriptions starting with `mystart` or ending with `endwith`.

    b. For **Service catalog items**:

    - **Service catalog items** – Choose to index service catalog items.
    - **Service catalog item attachments** – Choose to index service catalog item attachments.
    - **Active service catalog items** – Choose to index active service catalog items.
    - **Inactive service catalog items** – Choose to index inactive service catalog items.

- **Filter query** – Choose to include service catalog items based on a filter defined in your ServiceNow instance. Example filter queries include: *short_descriptionLIKEAccess^category=2809952237b1300054b6a3549dbe5dd4^EQ* *nameSTARTSWITHService^active=true^EQ*.
- **Include service catalog items based on short description filter** – Specify a regex pattern to include specific catalog items.

c. For **Incidents**:

- **Incidents** – Choose to index service incidents.
- **Incident attachments** – Choose to index incident attachments.
- **Active incidents** – Choose to index active incidents.
- **Inactive incidents** – Choose to index inactive incidents.
- **Active incident type** – Choose between **All incidents**, **Open incidents**, **Open - unassigned incidents**, and **Resolved incidents**, depending on your use case.
- **Filter query** – Choose to include incidents based on a filter defined in your ServiceNow instance. Example filter queries include: *short_descriptionLIKETest^urgency=3^state=1^EQ*, and *priority=2^category=software^EQ* .
- **Include incidents based on short description filter** – Specify a regex pattern to include specific incidents.

d. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

e. In **Additional configuration – *optional***:

- **Attachment regex patterns** – Add regular expression patterns to include or exclude specific attached files of catalogs, knowledge articles, and incidents. You can add up to 100 patterns.

f. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

To extract audio transcriptions and video content, enable processing for the following file types:

g. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

13. For **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync** – Sync all content regardless of the previous sync status.
    - **New, modified, or deleted content sync** – Only sync new, modified, and deleted content.

14. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
15. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
16. **Field mappings** – A list of data source document attributes to map to your index fields.

    > **Note**
    >
    > Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

    > **Note**
    >
    > Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

    For more information, see Field mappings.

17. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to ServiceNow using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- ServiceNow configuration properties
- ServiceNow JSON schema
- ServiceNow JSON schema example

ServiceNow configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has the following sub-property: `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-property: `hostUrl`, `authType`.	Yes
`hostUrl`	The ServiceNow host URL. For example, *`your-domain.service-now.com`* .	`string`	Yes
`authType`	The type of authentication you are using, either `basicAuth` or `OAuth2`.	`string`	Yes
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.		
• `knowledgeArticle`	A list of ServiceNow objects that Amazon	`object`	Yes

Configuration	Description	Type	Required
• attachment • serviceCatalog • incident	Q crawls and maps the attributes of to Amazon Q index field names.	This property has the following sub-properties: indexFieldName , indexFieldType , dataSourceFieldName , and dateFieldFormat .	
indexFieldName	The field name of your ServiceNow pages and assets.	string	Yes
indexFieldType	The field type of your ServiceNow pages and assets.	string The allowed values are STRING, STRING_LIST , DATE, and LONG.	Yes
dataSourceFieldName	The data source field name of your ServiceNow pages and assets.	string	Yes
dateFieldFormat	The date format of your ServiceNow pages and assets.	string Specify the date format in the form yyyy-MM-dd'T'HH:mm:ss'Z'	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties. • applyACLForKnowledgeArticle • applyACLForServiceCatalog • applyACLForIncident • isCrawlKnowledgeArticle • isCrawlKnowledgeArticleAttachment • includePublicArticlesOnly • knowledgeArticleFilter • knowledgeArticleTitleRegExp • isCrawlServiceCatalog	Yes

Configuration	Description	Type	Required
		• isCrawlServiceCatalogAttachment • isCrawlActiveServiceCatalog • isCrawlInactiveServiceCatalog • serviceCatalogQueryFilter • serviceCatalogTitleRegExp • isCrawlIncident • isCrawlIncidentAttachment • isCrawlActiveIncident • isCrawlInactiveIncident • incidentStateType • incidentQueryFilter • incidentTitleRegExp	

Configuration	Description	Type	Required
		• `maxFileSizeInMegaBytes` • `inclusionFileTypePatterns` • `exclusionFileTypePatterns` • `inclusionFileNamePatterns` • `exclusionFileNamePatterns`	
`maxFileSizeInMegaBytes`	Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string`	No

Configuration	Description	Type	Required
• knowledgeArticleFilter • incidentQueryFilter • serviceCatalogQueryFilter	Specify specific knowledge articles, incident queries, and service catalog queries to crawl.	string	No
incidentStateType	Specify incidents to crawl by state type: whether Open, Open - Unassigned , Resolved, or All.	array (string)	No
• knowledgeArticleTitleRegExp • serviceCatalogTitleRegExp • incidentTitleRegExp	A list of regular expression patterns to include and exclude specific files in your ServiceNow data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.	string	No

Configuration	Description	Type	Required
• `exclusionFileTypePatterns` • `exclusionFileNamePatterns`	A list of regular expression patterns to exclude specific content in your ServiceNow data source. Content that matches the patterns are excluded from the index. Content that doesn't match the patterns are included in the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array (string)`	No

Configuration	Description	Type	Required
• `inclusionFileTypePatterns` • `inclusionFileNamePatterns`	A list of regular expression patterns to include specific content in your ServiceNow data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array (string)`	No

Configuration	Description	Type	Required
• isCrawlKnowledgeArticle • isCrawlKnowledgeArticleAttachment • includePublicArticlesOnly • isCrawlServiceCatalog • isCrawlServiceCatalogAttachment • isCrawlActiveServiceCatalog • isCrawlInactiveServiceCatalog • isCrawlIncident • isCrawlIncidentAttachment • isCrawlActiveIncident • isCrawlInactiveIncident	Specify `true` to index ServiceNow knowledge articles, service catalogs, incidents, and attachments and their ACLs.	`boolean`	No

Configuration	Description	Type	Required
• `applyACLFor KnowledgeArticle` • `applyACLFor ServiceCatalog` • `applyACLFor Incident`			
`type`	The type of data source. We recommend that you use `SERVICENOWV2` as your data source type.	`string` Valid values are `SERVICENOWV2` and `SERVICENOW` .	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information,	`boolean`	No

Configuration	Description	Type	Required
	see Identity crawler.		
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required

`secretARN`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your ServiceNow.	`string`
		
		The secret must contain a JSON structure with the following keys:
		
		`{ "username": "user name", "password": "password" }`
		
		If you use OAuth2 authentication, your secret must contain a JSON structure with the following keys:
		
		`{ "username": "user name", "password": "password" , "clientId": "client id", "clientSecret": "client secret" }`
			Yes

`version`	The version of the template that's currently supported.	`string`	No

ServiceNow JSON schema

The following is the ServiceNow JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["SERVICENOWV2", "SERVICENOW"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FORCED_FULL_CRAWL", "FULL_CRAWL"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "hostUrl": {
              "type": "string",
              "pattern": "^(?!(^(https?|ftp|file):\\/\\/))[a-z0-9-]+(.service-
now.com|.servicenowservices.com)$",
              "minLength": 1,
              "maxLength": 2048
            },
```

```
            "authType": {
              "type": "string",
              "enum": ["basicAuth", "OAuth2"]
            },
            "servicenowInstanceVersion": {
              "type": "string",
              "enum": ["Tokyo", "Sandiego", "Rome", "Vancouver", "Others"]
            }
          },
          "required": ["hostUrl", "authType", "servicenowInstanceVersion"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "knowledgeArticle": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "STRING_LIST"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
```

```
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "attachment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "LONG", "DATE", "STRING_LIST"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "serviceCatalog": {
```

```
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "STRING_LIST"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        },
        "incident": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE", "STRING_LIST"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "isCrawlKnowledgeArticle": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
```

```
        "isCrawlKnowledgeArticleAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "includePublicArticlesOnly": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "knowledgeArticleFilter": {
          "type": "string"
        },
        "incidentQueryFilter": {
          "type": "string"
        },
        "serviceCatalogQueryFilter": {
          "type": "string"
        },
        "isCrawlServiceCatalog": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlServiceCatalogAttachment": {
          "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlActiveServiceCatalog": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlInactiveServiceCatalog": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlIncident": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlIncidentAttachment": {
          "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlActiveIncident": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlInactiveIncident": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "applyACLForKnowledgeArticle": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "applyACLForServiceCatalog": {
          "anyOf": [
```

```
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "applyACLForIncident": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "incidentStateType": {
          "type": "array",
          "items": {
            "type": "string",
            "enum": ["Open", "Open - Unassigned", "Resolved", "All"]
          }
        },
        "knowledgeArticleTitleRegExp": {
          "type": "string"
        },
        "serviceCatalogTitleRegExp": {
          "type": "string"
        },
        "incidentTitleRegExp": {
          "type": "string"
        },
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
```

```
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    },
    "required": [
```

```
      "type",
      "syncMode",
      "secretArn",
      "connectionConfiguration",
      "repositoryConfigurations",
      "additionalProperties"
    ]
  }
}
```

ServiceNow JSON schema example

The following is the ServiceNow JSON schema example:

```
{
  "type": "SERVICENOWV2",
  "syncMode": "FULL_CRAWL",
  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-servicenow-
secret",
  "enableIdentityCrawler": "true",
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "hostUrl": "mycompany.service-now.com",
      "authType": "basicAuth",
      "servicenowInstanceVersion": "Tokyo"
    }
  },
  "repositoryConfigurations": {
    "knowledgeArticle": {
      "fieldMappings": [
        {
          "indexFieldName": "article_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "attachment": {
      "fieldMappings": [
        {
          "indexFieldName": "attachment_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
```

```
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "serviceCatalog": {
      "fieldMappings": [
        {
          "indexFieldName": "catalog_item_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    },
    "incident": {
      "fieldMappings": [
        {
          "indexFieldName": "incident_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    }
  },
  "additionalProperties": {
    "maxFileSizeInMegaBytes": "50",
    "isCrawlKnowledgeArticle": "true",
    "isCrawlKnowledgeArticleAttachment": "true",
    "includePublicArticlesOnly": "false",
    "knowledgeArticleFilter": "filter_condition",
    "incidentQueryFilter": "incident_condition",
    "serviceCatalogQueryFilter": "service_catalog_condition",
    "isCrawlServiceCatalog": "true",
    "isCrawlServiceCatalogAttachment": "true",
    "isCrawlActiveServiceCatalog": "true",
    "isCrawlInactiveServiceCatalog": "false",
    "isCrawlIncident": "true",
    "isCrawlIncidentAttachment": "false",
    "isCrawlActiveIncident": "true",
    "isCrawlInactiveIncident": "false",
    "applyACLForKnowledgeArticle": "true",
    "applyACLForServiceCatalog": "true",
    "applyACLForIncident": "true",
```

```
    "incidentStateType": ["Open", "Resolved"],
    "knowledgeArticleTitleRegExp": ".*",
    "serviceCatalogTitleRegExp": ".*",
    "incidentTitleRegExp": ".*",
    "inclusionFileTypePatterns": ["*.pdf", "*.docx"],
    "exclusionFileTypePatterns": ["*.tmp"],
    "inclusionFileNamePatterns": ["important-*"],
    "exclusionFileNamePatterns": ["temporary-*"],
    "enableDeletionProtection": "false",
    "deletionProtectionThreshold": "15"
  }
}
```

Connecting Amazon Q Business to ServiceNow using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- ServiceNow configuration properties
- ServiceNow JSON schema for using the configuration property with AWS CloudFormation
- ServiceNow YAML schema for using the configuration property with AWS CloudFormation

ServiceNow configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has the following sub-	Yes

Configuration	Description	Type	Required
		property: `repositoryEndpointMetadata` .	
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-property: `hostUrl`, `authType`.	Yes
`hostUrl`	The ServiceNow host URL. For example, *`your-domain.service-now.com`* .	`string`	Yes
`authType`	The type of authentication you are using, either `basicAuth` or `OAuth2`.	`string`	Yes
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.		

Configuration	Description	Type	Required
• knowledgeArticle • attachment • serviceCatalog • incident	A list of ServiceNow objects that Amazon Q crawls and maps the attributes of to Amazon Q index field names.	object This property has the following sub-properties: indexFieldName , indexFieldType , dataSourceFieldName , and dateFieldFormat .	Yes
indexFieldName	The field name of your ServiceNow pages and assets.	string	Yes
indexFieldType	The field type of your ServiceNow pages and assets.	string The allowed values are STRING, STRING_LIST , DATE, and LONG.	Yes
dataSourceFieldName	The data source field name of your ServiceNow pages and assets.	string	Yes
dateFieldFormat	The date format of your ServiceNow pages and assets.	string Specify the date format in the form yyyy-MM-dd'T'HH:mm:ss'Z'	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties. • applyACLForKnowledgeArticle • applyACLForServiceCatalog • applyACLForIncident • isCrawlKnowledgeArticle • isCrawlKnowledgeArticleAttachment • includePublicArticlesOnly • knowledgeArticleFilter • knowledgeArticleTitleRegExp • isCrawlServiceCatalog	Yes

Configuration	Description	Type	Required
		• isCrawlServiceCatalogAttachment • isCrawlActiveServiceCatalog • isCrawlInactiveServiceCatalog • serviceCatalogQueryFilter • serviceCatalogTitleRegExp • isCrawlIncident • isCrawlIncidentAttachment • isCrawlActiveIncident • isCrawlInactiveIncident • incidentStateType • incidentQueryFilter • incidentTitleRegExp	

Configuration	Description	Type	Required
		• `maxFileSizeInMegaBytes` • `inclusionFileTypePatterns` • `exclusionFileTypePatterns` • `inclusionFileNamePatterns` • `exclusionFileNamePatterns`	
`maxFileSizeInMegaBytes`	Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string`	No

Configuration	Description	Type	Required
• `knowledgeArticleFilter` • `incidentQueryFilter` • `serviceCatalogQueryFilter`	Specify specific knowledge articles, incident queries, and service catalog queries to crawl.	`string`	No
`incidentStateType`	Specify incidents to crawl by state type: whether `Open`, `Open - Unassigned`, `Resolved`, or `All`.	`array (string)`	No
• `knowledgeArticleTitleRegExp` • `serviceCatalogTitleRegExp` • `incidentTitleRegExp`	A list of regular expression patterns to include and exclude specific files in your ServiceNow data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence and the file isn't included in the index.	`string`	No

Configuration	Description	Type	Required
• `exclusionFileTypePatterns` • `exclusionFileNamePatterns`	A list of regular expression patterns to exclude specific content in your ServiceNow data source. Content that matches the patterns are excluded from the index. Content that doesn't match the patterns are included in the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array (string)`	No

Configuration	Description	Type	Required
• `inclusionFileTypePatterns` • `inclusionFileNamePatterns`	A list of regular expression patterns to include specific content in your ServiceNow data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array (string)`	No

Configuration	Description	Type	Required
• `isCrawlKnowledgeArticle` • `isCrawlKnowledgeArticleAttachment` • `includePublicArticlesOnly` • `isCrawlServiceCatalog` • `isCrawlServiceCatalogAttachment` • `isCrawlActiveServiceCatalog` • `isCrawlInactiveServiceCatalog` • `isCrawlIncident` • `isCrawlIncidentAttachment` • `isCrawlActiveIncident` • `isCrawlInactiveIncident`	Specify `true` to index ServiceNow knowledge articles, service catalogs, incidents, and attachments and their ACLs.	`boolean`	No

Configuration	Description	Type	Required
• applyACLFor KnowledgeArticle • applyACLFor ServiceCatalog • applyACLFor Incident			
type	The type of data source. We recommend that you use SERVICENOWV2 as your data source type.	string Valid values are SERVICENOWV2 and SERVICENOW .	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	`true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to specific documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information,	`boolean`	No

Configuration	Description	Type	Required
	see Identity crawler.		
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	string You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required

`secretARN`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your ServiceNow.	`string`
		
		The secret must contain a JSON structure with the following keys:
		
		`{ "username": "user name", "password": "password" }`
		
		If you use OAuth2 authentication, your secret must contain a JSON structure with the following keys:
		
		`{ "username": "user name", "password": "password" , "clientId": "client id", "clientSecret": "client secret" }`
			Yes

`version`	The version of the template that's currently supported.	`string`	No

ServiceNow JSON schema for using the configuration property with AWS CloudFormation

The following is the ServiceNow JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- ServiceNow JSON schema for using the configuration property with AWS CloudFormation
- ServiceNow JSON schema example for using the configuration property with AWS CloudFormation

ServiceNow JSON schema for using the configuration property with AWS CloudFormation

The following is the ServiceNow JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "enum": ["SERVICENOWV2", "SERVICENOW"]
    },
    "syncMode": {
      "type": "string",
      "enum": ["FORCED_FULL_CRAWL", "FULL_CRAWL"]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
```

```
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "hostUrl": {
              "type": "string",
              "pattern": "^(?!(^(https?|ftp|file):\\/\\/))[a-z0-9-]+(.service-
now.com|.servicenowservices.com)$",
              "minLength": 1,
              "maxLength": 2048
            },
            "authType": {
              "type": "string",
              "enum": ["basicAuth", "OAuth2"]
            }
          },
          "required": ["hostUrl", "authType"]
        }
      },
      "required": ["repositoryEndpointMetadata"]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "knowledgeArticle": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "STRING_LIST"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
```

```
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": ["fieldMappings"]
    },
    "attachment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "LONG", "DATE", "STRING_LIST"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
```

```
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "serviceCatalog": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE", "STRING_LIST"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      },
      "incident": {
        "type": "object",
```

```
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "DATE", "STRING_LIST"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": ["fieldMappings"]
        }
      }
    },
    "additionalProperties": {
      "type": "object",
      "properties": {
        "maxFileSizeInMegaBytes": {
          "type": "string"
        },
        "isCrawlKnowledgeArticle": {
          "anyOf": [
            {
```

```
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "isCrawlKnowledgeArticleAttachment": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "includePublicArticlesOnly": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "knowledgeArticleFilter": {
        "type": "string"
      },
      "incidentQueryFilter": {
        "type": "string"
      },
      "serviceCatalogQueryFilter": {
        "type": "string"
      },
      "isCrawlServiceCatalog": {
        "anyOf": [
          {
            "type": "boolean"
          },
```

```
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlServiceCatalogAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlActiveServiceCatalog": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlInactiveServiceCatalog": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlIncident": {
          "anyOf": [
            {
              "type": "boolean"
            },
```

```
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlIncidentAttachment": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlActiveIncident": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "isCrawlInactiveIncident": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "applyACLForKnowledgeArticle": {
          "anyOf": [
            {
              "type": "boolean"
            },
```

```
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "applyACLForServiceCatalog": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "applyACLForIncident": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "incidentStateType": {
          "type": "array",
          "items": {
            "type": "string",
            "enum": ["Open", "Open - Unassigned", "Resolved", "All"]
          }
        },
        "knowledgeArticleTitleRegExp": {
          "type": "string"
        },
        "serviceCatalogTitleRegExp": {
          "type": "string"
        },
        "incidentTitleRegExp": {
          "type": "string"
        },
```

```
        "inclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFileNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    },
    "version": {
```

```
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    },
    "required": [
      "type",
      "syncMode",
      "secretArn",
      "connectionConfiguration",
      "repositoryConfigurations",
      "additionalProperties"
    ]
  }
}
```

ServiceNow JSON schema example for using the configuration property with AWS CloudFormation

The following is the ServiceNow JSON schema example for the configuration property for CloudFormation

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation SERVICENOW Data Source Template",
  "Resources": {
    "DataSourceServiceNow": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MyServiceNowDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "SERVICENOWV2",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-
servicenow-secret",
          "enableIdentityCrawler": "true",
          "connectionConfiguration": {
            "repositoryEndpointMetadata": {
```

```
            "hostUrl": "mycompany.service-now.com",
            "authType": "basicAuth",
          }
        },
        "repositoryConfigurations": {
          "knowledgeArticle": {
            "fieldMappings": [
              {
                "indexFieldName": "article_id",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          },
          "attachment": {
            "fieldMappings": [
              {
                "indexFieldName": "attachment_id",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          },
          "serviceCatalog": {
            "fieldMappings": [
              {
                "indexFieldName": "catalog_item_id",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
          },
          "incident": {
            "fieldMappings": [
              {
                "indexFieldName": "incident_id",
                "indexFieldType": "STRING",
                "dataSourceFieldName": "id",
                "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            ]
```

```
            }
          },
          "additionalProperties": {
            "maxFileSizeInMegaBytes": "50",
            "isCrawlKnowledgeArticle": "true",
            "isCrawlKnowledgeArticleAttachment": "true",
            "includePublicArticlesOnly": "false",
            "knowledgeArticleFilter": "filter_condition",
            "incidentQueryFilter": "incident_condition",
            "serviceCatalogQueryFilter": "service_catalog_condition",
            "isCrawlServiceCatalog": "true",
            "isCrawlServiceCatalogAttachment": "true",
            "isCrawlActiveServiceCatalog": "true",
            "isCrawlInactiveServiceCatalog": "false",
            "isCrawlIncident": "true",
            "isCrawlIncidentAttachment": "false",
            "isCrawlActiveIncident": "true",
            "isCrawlInactiveIncident": "false",
            "applyACLForKnowledgeArticle": "true",
            "applyACLForServiceCatalog": "true",
            "applyACLForIncident": "true",
            "incidentStateType": ["Open", "Resolved"],
            "knowledgeArticleTitleRegExp": ".*",
            "serviceCatalogTitleRegExp": ".*",
            "incidentTitleRegExp": ".*",
            "inclusionFileTypePatterns": ["*.pdf", "*.docx"],
            "exclusionFileTypePatterns": ["*.tmp"],
            "inclusionFileNamePatterns": ["important-*"],
            "exclusionFileNamePatterns": ["temporary-*"],
            "enableDeletionProtection": "false",
            "deletionProtectionThreshold": "15"
          }
        }
      }
    }
  }
}
```

ServiceNow YAML schema for using the configuration property with AWS CloudFormation

The following is the ServiceNow YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- ServiceNow YAML schema for using the configuration property with AWS CloudFormation
- ServiceNow YAML schema example for using the configuration property with AWS CloudFormation

ServiceNow YAML schema for using the configuration property with AWS CloudFormation

The following is the ServiceNow YAML schema for the configuration property for CloudFormation.

```
type: object
properties:
  type:
    type: string
    enum:
      - SERVICENOWV2
      - SERVICENOW
  syncMode:
    type: string
    enum:
      - FORCED_FULL_CRAWL
      - FULL_CRAWL
  secretArn:
    type: string
    minLength: 20
    maxLength: 2048
  enableIdentityCrawler:
    anyOf:
      - type: boolean
      - type: string
        enum:
          - "true"
          - "false"
  connectionConfiguration:
    type: object
    properties:
      repositoryEndpointMetadata:
        type: object
        properties:
          hostUrl:
            type: string
            pattern: "^(?!(^(https?|ftp|file):\\/\\/))[a-z0-9-]+(.service-
now.com|.servicenowservices.com)$"
```

```
            minLength: 1
            maxLength: 2048
          authType:
            type: string
            enum:
              - basicAuth
              - OAuth2
        required:
          - hostUrl
          - authType
    required:
      - repositoryEndpointMetadata
  repositoryConfigurations:
    type: object
    properties:
      knowledgeArticle:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - DATE
                    - STRING_LIST
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
        required:
          - fieldMappings
      attachment:
        type: object
```

```
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - LONG
                    - DATE
                    - STRING_LIST
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
                  type: string
                  pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
              required:
                - indexFieldName
                - indexFieldType
                - dataSourceFieldName
          required:
            - fieldMappings
      serviceCatalog:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - DATE
                    - STRING_LIST
                dataSourceFieldName:
                  type: string
```

```
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
    incident:
      type: object
      properties:
        fieldMappings:
          type: array
          items:
            type: object
            properties:
              indexFieldName:
                type: string
              indexFieldType:
                type: string
                enum:
                  - STRING
                  - DATE
                  - STRING_LIST
              dataSourceFieldName:
                type: string
              dateFieldFormat:
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
additionalProperties:
  type: object
  properties:
    maxFileSizeInMegaBytes:
      type: string
    isCrawlKnowledgeArticle:
      anyOf:
        - type: boolean
```

```
          - type: string
            enum:
              - "true"
              - "false"
      isCrawlKnowledgeArticleAttachment:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      includePublicArticlesOnly:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      knowledgeArticleFilter:
        type: string
      incidentQueryFilter:
        type: string
      serviceCatalogQueryFilter:
        type: string
      isCrawlServiceCatalog:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      isCrawlServiceCatalogAttachment:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      isCrawlActiveServiceCatalog:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
```

```
        - "false"
    isCrawlInactiveServiceCatalog:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    isCrawlIncident:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    isCrawlIncidentAttachment:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    isCrawlActiveIncident:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    isCrawlInactiveIncident:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    applyACLForKnowledgeArticle:
      anyOf:
        - type: boolean
        - type: string
          enum:
            - "true"
            - "false"
    applyACLForServiceCatalog:
```

```
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      applyACLForIncident:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
      incidentStateType:
        type: array
        items:
          type: string
          enum:
            - Open
            - Open - Unassigned
            - Resolved
            - All
      knowledgeArticleTitleRegExp:
        type: string
      serviceCatalogTitleRegExp:
        type: string
      incidentTitleRegExp:
        type: string
      inclusionFileTypePatterns:
        type: array
        items:
          type: string
      exclusionFileTypePatterns:
        type: array
        items:
          type: string
      inclusionFileNamePatterns:
        type: array
        items:
          type: string
      exclusionFileNamePatterns:
        type: array
        items:
          type: string
```

```
      enableDeletionProtection:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - "true"
              - "false"
        default: false
      deletionProtectionThreshold:
        type: string
        default: "15"
    required: []
  version:
    type: string
    anyOf:
      - pattern: "1.0.0"
  required:
    - type
    - syncMode
    - secretArn
    - connectionConfiguration
    - repositoryConfigurations
    - additionalProperties
```

ServiceNow YAML schema example for using the configuration property with AWS CloudFormation

The following is the ServiceNow YAML example for the Configuration property for CloudFormation:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: CloudFormation SERVICENOW Data Source Template
Resources:
  DataSourceServiceNow:
    Type: AWS::QBusiness::DataSource
    Properties:
      ApplicationId: app12345-1234-1234-1234-123456789012
      IndexId: indx1234-1234-1234-1234-123456789012
      DisplayName: MyServiceNowDataSource
      RoleArn: arn:aws:iam::123456789012:role/qbusiness-data-source-role
      Configuration:
        type: SERVICENOWV2
        syncMode: FULL_CRAWL
```

```
        secretArn: arn:aws:secretsmanager:us-west-2:123456789012:secret:my-servicenow-
secret
        enableIdentityCrawler: "true"
        connectionConfiguration:
          repositoryEndpointMetadata:
            hostUrl: mycompany.service-now.com
            authType: basicAuth
        repositoryConfigurations:
          knowledgeArticle:
            fieldMappings:
              - indexFieldName: article_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
          attachment:
            fieldMappings:
              - indexFieldName: attachment_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
          serviceCatalog:
            fieldMappings:
              - indexFieldName: catalog_item_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
          incident:
            fieldMappings:
              - indexFieldName: incident_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
        additionalProperties:
          maxFileSizeInMegaBytes: "50"
          isCrawlKnowledgeArticle: "true"
          isCrawlKnowledgeArticleAttachment: "true"
          includePublicArticlesOnly: "false"
          knowledgeArticleFilter: filter_condition
          incidentQueryFilter: incident_condition
          serviceCatalogQueryFilter: service_catalog_condition
          isCrawlServiceCatalog: "true"
          isCrawlServiceCatalogAttachment: "true"
          isCrawlActiveServiceCatalog: "true"
          isCrawlInactiveServiceCatalog: "false"
```

```
        isCrawlIncident: "true"
        isCrawlIncidentAttachment: "false"
        isCrawlActiveIncident: "true"
        isCrawlInactiveIncident: "false"
        applyACLForKnowledgeArticle: "true"
        applyACLForServiceCatalog: "true"
        applyACLForIncident: "true"
        incidentStateType:
          - Open
          - Resolved
        knowledgeArticleTitleRegExp: ".*"
        serviceCatalogTitleRegExp: ".*"
        incidentTitleRegExp: ".*"
        inclusionFileTypePatterns:
          - "*.pdf"
          - "*.docx"
        exclusionFileTypePatterns:
          - "*.tmp"
        inclusionFileNamePatterns:
          - important-*
        exclusionFileNamePatterns:
          - temporary-*
        enableDeletionProtection: "false"
        deletionProtectionThreshold: "15"
```

How Amazon Q Business connector crawls ServiceNow ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an ServiceNow data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your ServiceNow instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end user's document access level.

> **Note**
>
> Amazon Q Business supports:
>
> - Role-based, static ACLs for Service Catalogs

- Role-based, static ACLs for Knowledge Bases
- Role-based, static ACLs for Incidents

Amazon Q Business does not honor limitations set by ServiceNow's advanced ACLs on documents.

The group and user IDs are mapped as follows:

- `_group_ids` – Group IDs exist in ServiceNow on files where there are set access permissions. They're mapped from the role names of `sys_ids` in ServiceNow.
- `_user_id` – User IDs exist in ServiceNow on files where there are set access permissions. They're mapped from the user emails as the IDs in ServiceNow.

Important

To maintain secure access control for Amazon Q Business, each user must have a unique email address across all connected data sources.
In ServiceNow users can share an email address while having a different application-specific unique identifier. However, in Amazon Q Business email addresses act as unique identifiers. This means that if a document is shared with a particular user (for example, arnav_desai@example.com who is part of pentesters@example.com) on the basis of an application-specific unique ID, every other user who shares pentesters@example.com (for example, xiulan_wang@example.com and efua_owusu@example.com, both of whom are part of pentesters@example.com) can receive Amazon Q Business responses with content from a document that was shared only with Arnav. Similarly, content created by Arnav that only he should be able to access via Amazon Q Business chat responses, could also be part of Amazon Q Business chat responses for Xiulan and Efua, because they share the same email address.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

ServiceNow Online data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q ServiceNow connector supports the following entities and the associated reserved and custom attributes.

Supported entities and field mappings

- Knowledge articles
- Service catalog
- Attachments
- Incidents

Knowledge articles

Amazon Q supports crawling ServiceNow Online Knowledge articles and offers the following knowledge article field mappings.

ServiceNow field name	Index field name	Description	Data type
text	sn_ka_text	Custom	String
short_description	sn_ka_short_description	Custom	String
sys_created_on	_created_at	Default	Date
sys_updated_on	_last_updated_at	Default	Date
kb_category_name	_category	Default	String
sys_created_by	_authors	Default	String
sys_updated_by	sn_updatedBy	Custom	String
sys_id	sn_sys_id	Custom	String
published	sn_ka_publish_date	Custom	Date
workflow_state	sn_ka_workflow_state	Custom	String
kb_category	sn_ka_category	Custom	String
article_type	sn_ka_article_type	Custom	String
first_name	sn_ka_first_name	Custom	String
last_name	sn_ka_last_name	Custom	String
user_name	sn_ka_user_name	Custom	String
valid_to	sn_ka_valid_to	Custom	Date

ServiceNow field name	Index field name	Description	Data type
kb_knowledge_base	sn_ka_knowledge_base	Custom	String
number	sn_ka_number	Custom	String
url	sn_url	Custom	String
diplayUrl	_source_uri	Default	String
replacement_article	sn_ka_replacement_article	Custom	String
description	sn_ka_description	Custom	String
wiki	sn_ka_wiki	Custom	String
rating	sn_ka_rating	Custom	String
rating	sn_ka_rating	Custom	String
view_as_allowed	sn_ka_view_as_allowed	Custom	String
source	sn_ka_source	Custom	String
image	sn_ka_image	Custom	String
author	sn_ka_author	Custom	String
active	sn_ka_active	Custom	String
helpful_count	sn_ka_helpful_count	Custom	String
meta_description	sn_ka_meta_description	Custom	String
meta	sn_ka_meta	Custom	String

ServiceNow field name	Index field name	Description	Data type
topic	sn_ka_topic	Custom	String
roles	sn_ka_roles	Custom	String
disable_suggesting	sn_ka_disable_suggesting	Custom	String
use_count	sn_ka_use_count	Custom	String
flagged	sn_ka_flagged	Custom	String
disable_commenting	sn_ka_disable_commenting	Custom	String
retired	sn_ka_retired	Custom	String
display_attachments	sn_ka_display_attachments	Custom	String
taxonomy_topic	sn_ka_taxonomy_topic	Custom	String

Service catalog

Amazon Q supports crawling ServiceNow Online service catalogs and offers the following service catalog field mappings.

ServiceNow field name	Index field name	Description	Data type
description	sn_sc_description	Custom	String
short_description	sn_sc_short_description	Custom	String
sys_created_on	_created_at	Default	Date

ServiceNow field name	Index field name	Description	Data type
sys_updated_on	_last_updated_at	Default	Date
category_name	_category	Default	String
sys_created_by	_authors	Default	String list
sys_updated_by	sn_updated_by	Custom	String
sys_id	sn_sys_id	Custom	String
sc_catalogs	sn_sc_catalogs	Custom	String
sc_catalogs_name	sn_sc_catalogs_name	Custom	String
category	sn_sc_category	Custom	String
category_full_name	sn_sc_category	Custom	String
url	sn_url	Custom	String
displayUrl	_source_uri	Default	String
show_variable_help_on_load	sn_sc_show_var_help_on_load	Custom	String
no_order_now	sn_sc_no_order_now	Custom	String
sc_ic_version	sn_sc_sc_ic_version	Custom	String
delivery_time	sn_sc_deliver_time	Custom	String
published_ref	sn_sc_published_ref	Custom	String
price	sn_sc_price	Custom	String
recurring_frequency	sn_sc_recurring_frequency	Custom	String
sys_name	sn_sc_sys_name	Custom	String

ServiceNow field name	Index field name	Description	Data type
model	sn_sc_model	Custom	String
state	sn_sc_state	Custom	String
no_cart	sn_sc_no_cart	Custom	String
group	sn_sc_group	Custom	String
hide_sp	sn_sc_hide_sp	Custom	String
order	sn_sc_order	Custom	String
start_closed	sn_sc_start_closed	Custom	String
image	sn_sc_image	Custom	String
no_quantity	sn_sc_no_quantity	Custom	String
delivery_plan	sn_sc_delivery_plan	Custom	String
active	sn_sc_active	Custom	String
checked_out	sn_sc_checked_out	Custom	String
custom_cart	sn_sc_custom_cart	Custom	String
no_cart_v2	sn_sc_no_cart_v2	Custom	String
no_proceed_checkout	sn_sc_no_proceed_checkout	Custom	String
ignore_price	sn_sc_ignore_price	Custom	String
sys_update_name	sn_sc_sys_update_name	Custom	String
meta	sn_sc_meta	Custom	String
omit_price	sn_sc_omit_price	Custom	String

ServiceNow field name	Index field name	Description	Data type
name	sn_sc_name	Custom	String
mobile_hide_price	sn_sc_mobile_hide_price	Custom	String
no_wishlist_v2	sn_sc_no_wishlist_v2	Custom	String
preview	sn_sc_preview	Custom	String
type	sn_sc_type	Custom	String
access_type	sn_sc_access_type	Custom	String
roles	sn_sc_roles	Custom	String
icon	sn_sc_icon	Custom	String
mobile_picture	sn_sc_mobile_picture	Custom	String
availability	sn_sc_availability	Custom	String
mandatory_attachment	sn_sc_mandatory_attachment	Custom	String
request_method	sn_sc_request_method	Custom	String
visible_guide	sn_sc_visible_guide	Custom	String
visible_standalone	sn_sc_visible_standalone	Custom	String
no_order	sn_sc_no_order	Custom	String
vendor	sn_sc_vendor	Custom	String
no_attachment_v2	sn_sc_no_attachment_v2	Custom	String

ServiceNow field name	Index field name	Description	Data type
mobile_picture_type	sn_sc_mobile_picture_type	Custom	String
visible_bundle	sn_sc_visible_bundle	Custom	String
ordered_item_link	sn_sc_ordered_item_link	Custom	String
owner	sn_sc_owner	Custom	String
no_delivery_time_v2	sn_sc_no_delivery_time_v2	Custom	String
cost	sn_sc_cost	Custom	String
no_quantity_v2	sn_sc_no_quantity_v2	Custom	String
recurring_price	sn_sc_recurring_price	Custom	String
list_price	sn_sc_list_price	Custom	String
syst_tags	sn_sc_sys_tags	Custom	String
billable	sn_sc_billable	Custom	String
picture	sn_sc_picture	Custom	String
display_price_property	sn_sc_display_price_property	Custom	String
taxonomy_topic	sn_sc_taxonomy_topic	Custom	String
delivery_plain_script	sn_sc_delivery_plain_script	Custom	String
location	sn_sc_location	Custom	String

Attachments

Amazon Q supports crawling ServiceNow Online attachments and offers the following attachment field mappings.

ServiceNow field name	Index field name	Description	Data type
size_bytes	sn_file_size	Custom	Long (numeric)
file_name	sn_file_name	Custom	String
sys_mod_count	sn_sys_mod_count	Custom	String
average_image_color	sn_average_image_color	Custom	String
image_width	sn_image_width	Custom	String
sys_updated_on	_last_updated_at	Default	Date
sys_tags	sn_sys_tags	Custom	String
table_name	sn_table_name	Custom	String
sys_id	sn_sys_id	Custom	String
image_height	sn_image_height	Custom	String
sys_updated_by	sn_updated_by	Custom	String
content_type	sn_content_type	Custom	String
sys_created_on	_created_at	Default	Date
size_compressed	sn_size_compressed	Custom	String
compressed	sn_compressed	Custom	String
state	sn_state	Custom	String
table_sys_id	sn_table_sys_id	Custom	String

ServiceNow field name	Index field name	Description	Data type
chunk_size_bytes	sn_chunk_size_bytes	Custom	String
hash	sn_hash	Custom	String
sys_created_by	_authors	Default	String list
sys_updated_by	sn_updated_by	Custom	String
url	sn_url	Custom	String
displayUrl	_source_uri	Default	String

Incidents

Amazon Q supports crawling ServiceNow Online incidents and offers the following incident field mappings.

ServiceNow field name	Index field name	Description	Data type
short_description	sn_inc_short_description	Custom	String
description	sn_inc_description	Custom	String
sys_updated_on	_last_updated_at	Default	Date
number	sn_inc_number	Custom	String
sys_updated_by	sn_updatedBy	Custom	String
displayUrl	_source_uri	Default	String
opened_by	sn_inc_opened_by	Custom	String
sys_created_on	_created_at	Default	Date

ServiceNow field name	Index field name	Description	Data type
state	sn_inc_state	Custom	String
sys_created_by	_authors	Default	String list
business_impact	sn_inc_business_impact	Default	String
impact	sn_inc_business_impact	Custom	String
priority	sn_inc_priority	Custom	String
urgency	sn_inc_urgency	Custom	String
opened_at	an_inc_opened_at	Custom	String
business_duration	sn_inc_business_duration	Custom	String
caller_id	sn_inc_caller_id	Custom	String
resolved_at	sn_inc_resolved_at	Custom	String
category	sn_inc_category	Custom	String
subcategory	sn_inc_subcategory	Custom	String
close_code	sn_inc_close_code	Custom	String
assignment_group	sn_inc_assignment_group	Custom	String
close_notes	sn_inc_close_notes	Custom	String
displayUrl	_source_uri	Default	String
sys_class_name	sn_inc_sys_class_name	Custom	String

ServiceNow field name	Index field name	Description	Data type
parent_incident	an_inc_parent_incident	Custom	String
incident_state	sn_incident_state	Custom	String
company	sn_inc_company	Custom	String
assigned_to	sn_inc_assigned_to	Custom	String
hold_reason	an_inc_hold_reason	Custom	String
work_notes	sn_inc_work_notes	Custom	String
comments_and_work_notes	sn_inc_comments_and_work_notes	Custom	String
work_notes_list	sn_work_notes_list	Custom	String
comments	sn_inc_comments	Custom	String
sys_id	sn_inc_sys_id	Custom	String
url	sn_url	Custom	String
active	sn_inc_active	Custom	String
activity_due	sn_inc_activity_due	Custom	String
additional_assignee_list	sn_inc_additional_assign_list	Custom	String
approval	sn_inc_approval	Custom	String
approval_history	sn_inc_approval_history	Custom	String
approval_set	sn_inc_approval_set	Custom	Date

ServiceNow field name	Index field name	Description	Data type
business_service	sn_inc_business_service	Custom	String
closed_by	sn_inc_closed_by	Custom	String
cmdb_ci	sn_inc_cmdb_id	Custom	String
resolved_by	sn_inc_resolved_by	Custom	String
sys_domain	sn_inc_sys_domain	Custom	String
business_stc	sn_inc_business_stc	Custom	String
calendar_duration	sn_inc_calendar_duration	Custom	String
calendar_stc	sn_inc_calendar_stc	Custom	String
cause	sn_inc_cause	Custom	String
caused_by	sn_inc_caused_by	Custom	String
child_incidents	sn_inc_child_incidents	Custom	String
closed_at	sn_inc_closed_at	Custom	String
contact_type	sn_inc_contact_type	Custom	String
contract	sn_inc_contract	Custom	String
correlation_display	sn_inc_correlation_display	Custom	String
delivery_plan	sn_inc_delivery_plan	Custom	String
delivery_task	sn_inc_delivery_task	Custom	String

ServiceNow field name	Index field name	Description	Data type
due_date	sn_inc_due_date	Custom	String
escalation	sn_inc_escalation	Custom	String
expected_start	sn_inc_expected_start	Custom	String
follow_up	sn_inc_follow_up	Custom	String
group_list	sn_inc_group_list	Custom	String
knowledge	sn_inc_knowledge	Custom	String
location	sn_inc_location	Custom	String
made_sla	sn_inc_made_sla	Custom	String
notify	sn_inc_notify	Custom	String
order	sn_inc_order	Custom	String
origin_id	sn_inc_origin_id	Custom	String
origin_table	sn_inc_origin_table	Custom	String
parent	sn_inc_parent	Custom	String
problem_id	sn_inc_problem_id	Custom	String
reassignment_count	sn_inc_reassignment_count	Custom	String
repoen_count	sn_inc_reopen_count	Custom	String
reopened_by	sn_inc_reopened_by	Custom	String
reopened_time	sn_inc_reopened_time	Custom	String

ServiceNow field name	Index field name	Description	Data type
rfc	sn_inc_rfc	Custom	String
route_reason	sn_inc_route_reason	Custom	String
service_offering	sn_inc_service_offering	Custom	String
severity	sn_inc_severity	Custom	String
sla_due	sn_inc_sla_due	Custom	Date
task_effective_number	sn_inc_task_effective_number	Custom	String
time_worked	sn_inc_time_worked	Custom	Date
universal_request	sn_inc_universal_request	Custom	String
upon_approval	sn_inc_upon_approval	Custom	String
upon_reject	sn_inc_upon_reject	Custom	String
user_input	sn_inc_user_input	Custom	String
watch_list	sn_inc_watch_list	Custom	String
work_end	sn_inc_work_end	Custom	String
work_start	sn_inc_work_start	Custom	String

IAM role for Amazon Q Business ServiceNow Online connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
```

```
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
```

```
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
```

```
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
```

```
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the Amazon Q Business ServiceNow Online connector

The following table provides information about error codes you may see for the ServiceNow Online connector and suggested resolutions.

Error code	Error message	Suggested resolution
SRN-5001	Error validating credentials due to invalid client id or client secret or username or password.	Provide a valid client id/client secret/username/password.
SRN-5002	Error validating credentials due to invalid username or password.	Provide a valid username/password.
SRN-5003	Access token is empty or null.	Provide a non empty or non null access token.
SRN-5004	Client ID exceeded the allowed length.	Provide a valid Client ID.
SRN-5005	Client Secret exceeded the allowed length.	Provide a valid Client Secret.
SRN-5006	Password exceeded the allowed length.	Provide a valid Password.
SRN-5007	clientSecret contains non-printable Ascii characters.	Provide a valid clientSecret.

Error code	Error message	Suggested resolution
SRN-5008	clientId contains non-printable Ascii characters.	Provide a valid clientId.
SRN-5010	Error validating credentials due to invalid username or password.	Provide a valid username/password.
SRN-5011	Amazon Q can't connect to the ServiceNow server with the specified credentials.	Provide admin credentials and try your request again.
SRN-5014	ServiceNow instance is not available.	Check your ServiceNow instance before crawling.
SRN-5100	Client id should not be empty.	Provide a valid client id.
SRN-5101	Client secret should not be empty.	Provide a valid client secret.
SRN-5102	User name should not be empty.	Provide a valid username.
SRN-5103	Password should not be empty.	Provide a valid password.
SRN-5104	Auth type should not be empty.	Provide an auth Type.
SRN-5105	Incorrect auth type.	Auth type should be basicAuth or OAuth2.
SRN-5106	Host url should not be empty.	Provide a valid host url.

Error code	Error message	Suggested resolution
SRN-5120	crawlType should not be empty.	crawlType should be FORCED_FULL_CRAWL or FULL_CRAWL or CHANGE_LOG.
SRN-5122	isCrawlKnowledgeArticle should not be empty.	Provide valid isCrawlKnowledgeArticle.
SRN-5123	Invalid isCrawlKnowledgeArticle value.	isCrawlKnowledgeArticle should be true or false.
SRN-5124	isCrawlKnowledgeArticleAttachment should not be empty.	Provide valid isCrawlKnowledgeArticleAttachment.
SRN-5125	Invalid isCrawlKnowledgeArticleAttachment value.	isCrawlKnowledgeArticleAttachment should be true or false.
SRN-5126	isCrawlServiceCatalog should not be empty.	Provide valid isCrawlServiceCatalog.
SRN-5127	invalid isCrawlServiceCatalog value.	isCrawlServiceCatalog should be true or false.
SRN-5128	isCrawlServiceCatalogAttachment should not be empty.	Provide valid isCrawlServiceCatalogAttachment.
SRN-5129	Invalid isCrawlServiceCatalogAttachment value.	isCrawlServiceCatalogAttachment should be true or false.
SRN-5130	isCrawlIncident should not be empty.	Provide valid isCrawlIncident.
SRN-5131	invalid isCrawlIncident value.	isCrawlIncident should be true or false.

Error code	Error message	Suggested resolution
SRN-5132	isCrawlIncidentAttachment should not be empty.	Provide valid isCrawlIncidentAttachment.
SRN-5133	Invalid isCrawlIncidentAttachment value.	isCrawlIncidentAttachment should be true or false.
SRN-5134	Invalid incidentStateType.	Invalid incidentStateType. Incident State Type should be All, Open, Open - Unassigned or Resolved.
SRN-5135	applyACLForKnowledgeArticle should not be empty.	Provide valid applyACLForKnowledgeArticle.
SRN-5136	applyACLForServiceCatalog should not be empty.	Provide valid applyACLForServiceCatalog.
SRN-5137	applyACLForIncident should not be empty.	Provide valid applyACLForIncident.
SRN-5138	Invalid applyACLForKnowledgeArticle value.	applyACLForKnowledgeArticle should be true or false.
SRN-5139	Invalid applyACLForServiceCatalog value.	applyACLForServiceCatalog should be true or false.
SRN-5140	Invalid applyACLForIncident value.	applyACLForIncident should be true or false.
SRN-5141	invalid pattern :”file type pattern”	Provide valid patterns.

Error code	Error message	Suggested resolution
SRN-5142	includePublicArticlesOnly should not be empty.	Provide valid includePublicArticlesOnly.
SRN-5143	Invalid includePublicArticlesOnly value.	includePublicArticlesOnly should be true or false.
SRN-5144	Invalid URI.	Provide valid URI.
SRN-5145	isCrawlActiveServiceCatalog should not be empty.	Provide valid isCrawlActiveServiceCatalog.
SRN-5146	isCrawlInActiveServiceCatalog should not be empty.	Provide valid isCrawlInactiveServiceCatalog.
SRN-5147	isCrawlActiveIncident should not be empty.	Provide valid isCrawlActiveIncident.
SRN-5148	isCrawlInActiveIncident should not be empty.	Provide valid isCrawlInactiveIncident.
SRN-5149	Invalid isCrawlActiveServiceCatalog value.	isCrawlActiveServiceCatalog should be true or false.
SRN-5150	Invalid isCrawlInactiveServiceCatalog value.	isCrawlInactiveServiceCatalog should be true or false.
SRN-5151	Invalid isCrawlActiveIncident value.	isCrawlActiveIncident should be true or false.
SRN-5152	Invalid isCrawlInactiveIncident value.	isCrawlInactiveIncident should be true or false.

Error code	Error message	Suggested resolution
SRN-5153	servicenowInstance Version should not be empty.	Provide a valid servicenowInstance Version.
SRN-5154	The ServiceNow host name is invalid.	The ServiceNow host name should follow the format: example.service-now.com
SRN-5501	continuableInternalServerError.	Try again later.

Connecting Slack to Amazon Q Business

Slack is an enterprise communications app that lets users send messages and attachments through various public and private channels. You can connect your Slack instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the Slack connector
- Slack connector overview
- Prerequisites for connecting Amazon Q Business to Slack
- Setting up Slack for connecting to Amazon Q
- Connecting Amazon Q Business to Slack using the console
- Connecting Amazon Q Business to Slack using APIs
- Connecting Amazon Q Business to Slack using AWS CloudFormation
- How Amazon Q Business connector crawls Slack ACLs
- Slack data source connector field mappings
- IAM role for the Slack connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Slack connector

The Slack connector has the following known limitations:

- Due to API limitations, the Amazon Q Slack connector can only retrieve a maximum of 100 pages, with 100 files per page. Given this limitation, the Slack connector can only crawl a maximum of 10,000 files per channel.

Slack connector overview

The following table gives an overview of the Amazon Q Business Slack connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	Token based authentication
	Authentication credentials	• Slack workspace ID • Either Slack Bot token or User token User token lets you make API requests on behalf of the user. Bot token lets you make API requests as a Slack bot.
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes

Category	Feature	Support
	VPC	Yes
Crawl features	**Custom metadata**	No
	Entities	Yes. The following entities are supported: • Public channels • Private channels • Group messages • Private messages • Bot messages • Archived messages See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports default and custom field mappings. For more information, see Field mappings.

Category	Feature	Support
	Filters	Yes. The following filters are supported : • Crawl public channel • Crawl private channel • Crawl group messages • Crawl private messages • Crawl channel by type • Crawl channel by name • Including and excluding content by file type • Including and excluding content based on file name
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.
	Crawled as a document	• Each message • Each message attachment • Each channel post

Prerequisites for connecting Amazon Q Business to Slack

Before you begin, make sure that you have completed the following prerequisites.

In Slack, make sure you have:

- Created a Slack Bot User OAuth token or Slack User OAuth token. You can choose either token to connect Amazon Q to your Slack data source. See Slack documentation on access tokens for more information.

> **Note**
>
> If you use the bot token as part of your Slack credentials, you cannot index direct messages and group messages. You must add the bot token to the channel you want to index.

- Noted your Slack workspace team ID from your Slack workspace main page URL. For example, *`https://app.slack.com/client/T0123456789/...`* where *`T0123456789`* is the team ID.
- Added the required OAuth scopes/ read permissions. See Setting up Slack for more details.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Slack authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

> **Note**
>
> For more information on connecting Slack to Amazon Q Business, see Unlock the knowledge in your Slack workspace with Slack connector for Amazon Q Business in the *AWS Machine Learning Blog*.

Setting up Slack for connecting to Amazon Q

Before you connect Slack to Amazon Q, you need to create and retrieve the Slack credentials you will use to connect Slack to Amazon Q. You will also need to add any permissions needed by Slack to connect to Amazon Q.

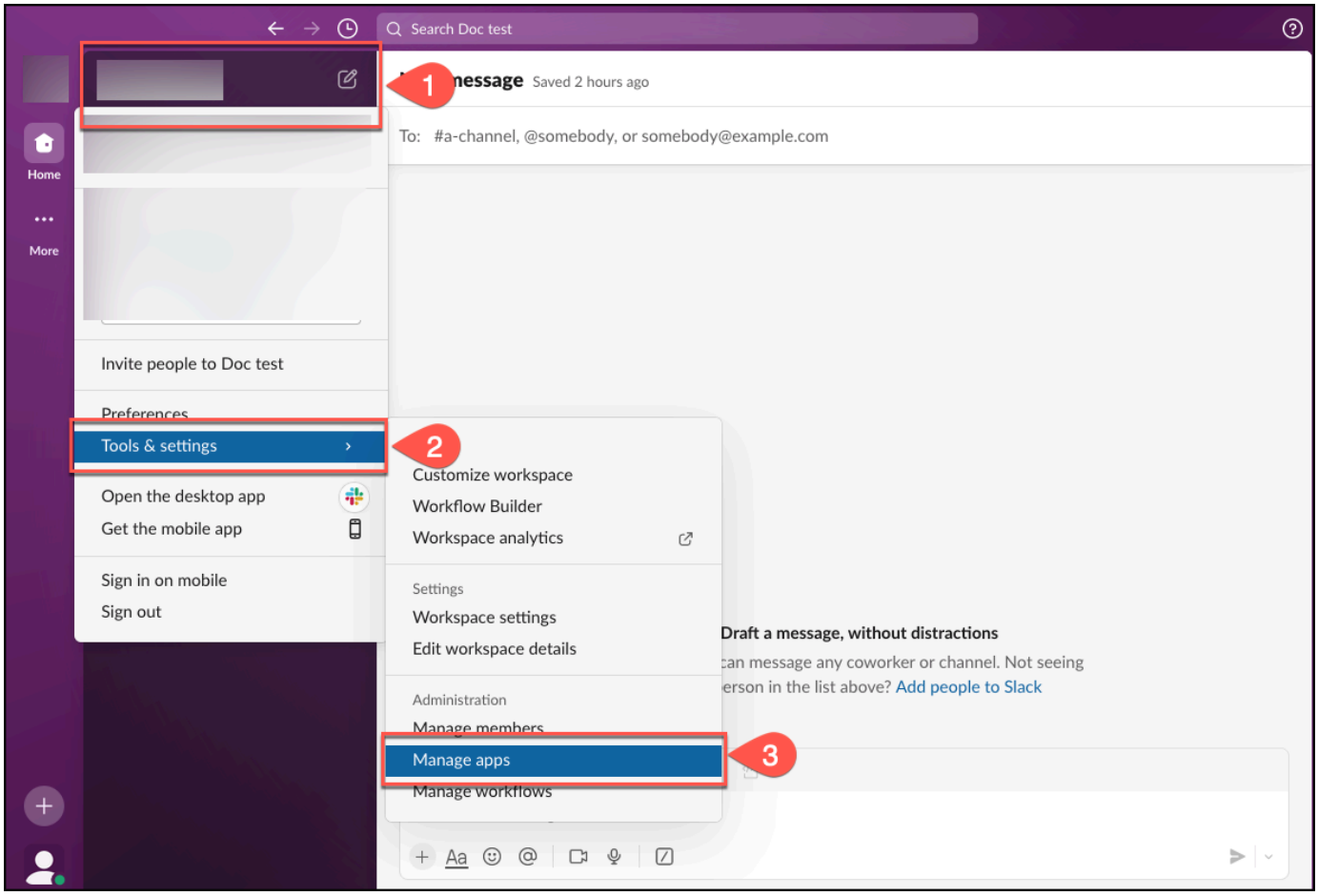
The following procedure gives you an overview of how to configure Slack for connecting with Amazon Q.

Configuring Slack authentication for Amazon Q

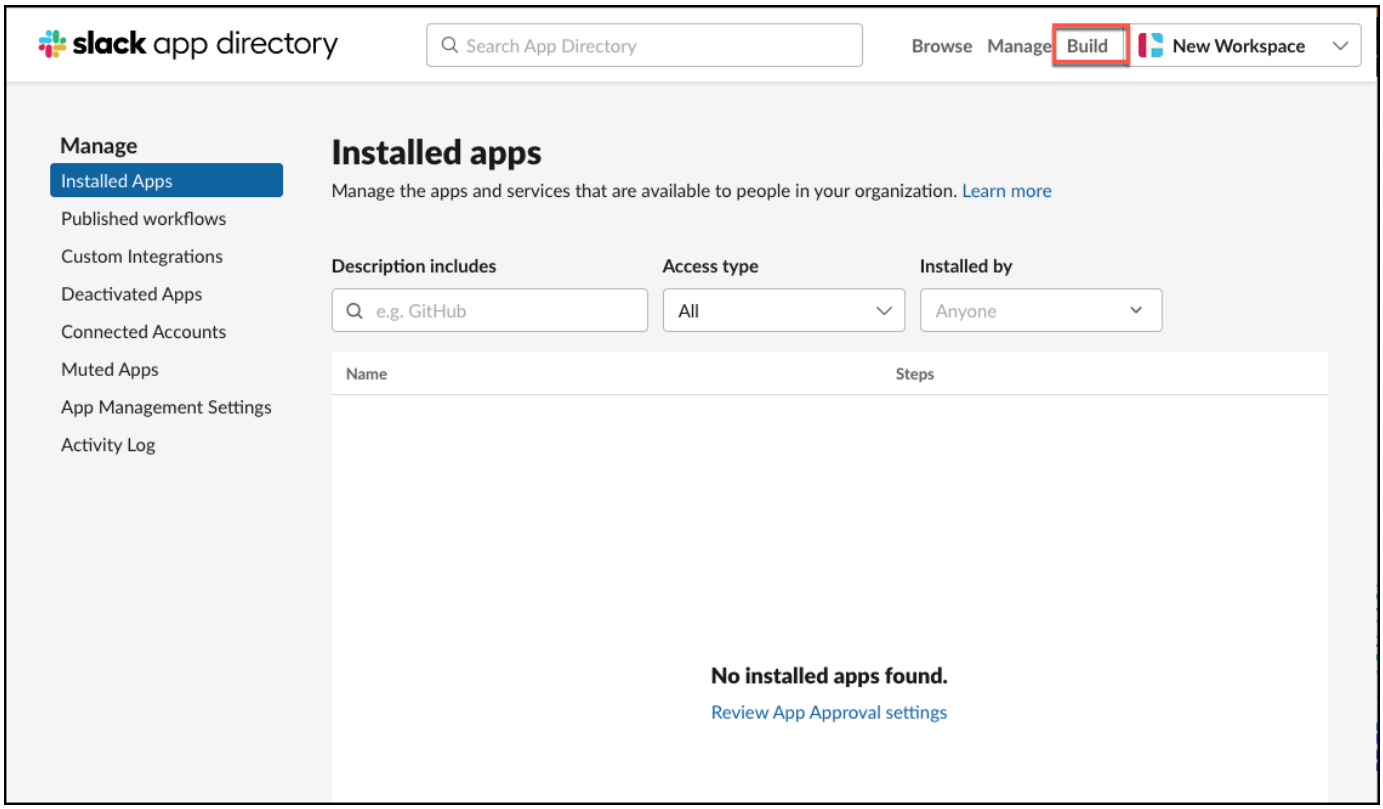
1. Log in to your Slack account and sign into your Slack workspace.

> **Note**
>
> To configure Slack for Amazon Q, you must be an admin user in the Slack account.

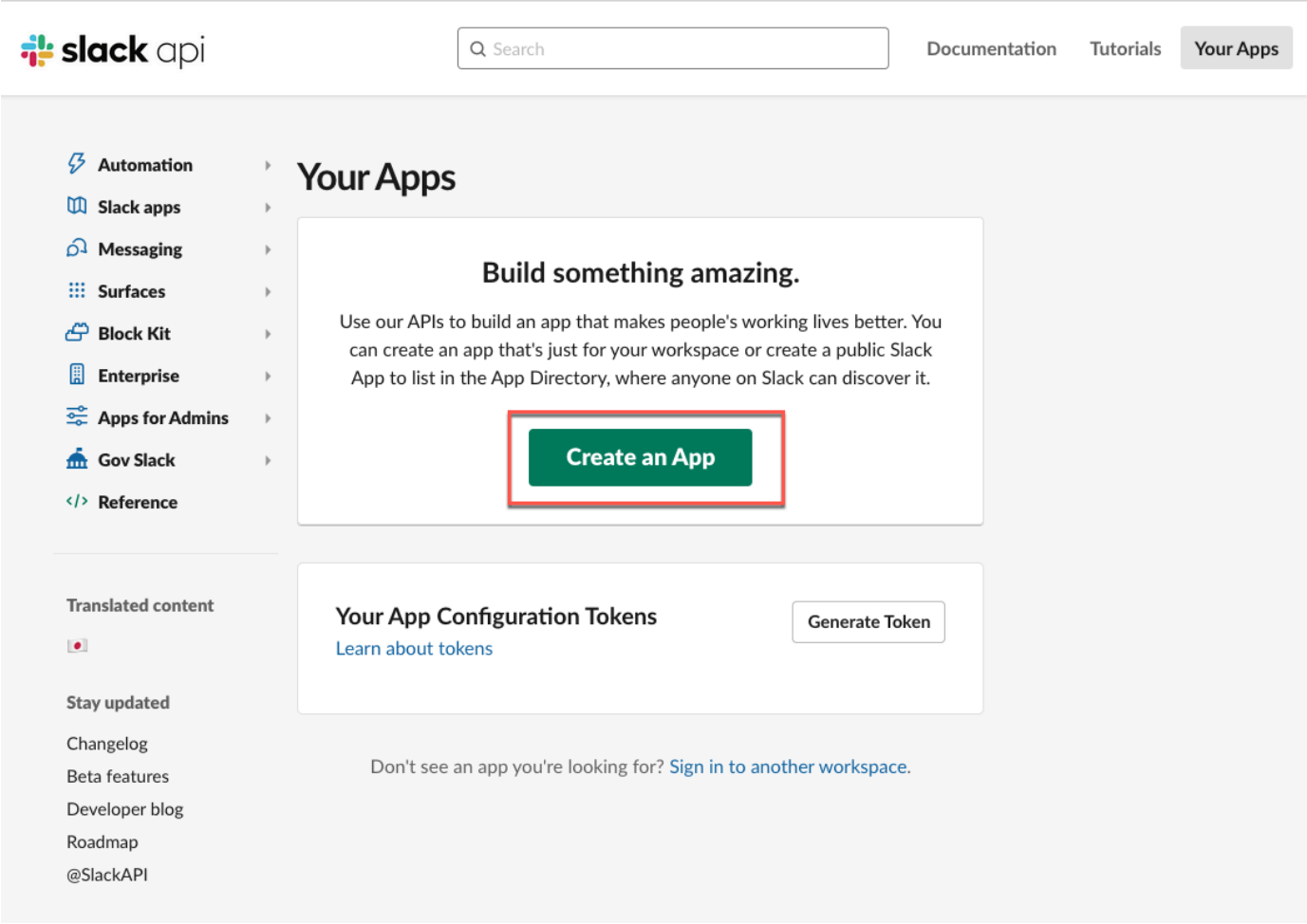
2. From the workspace menu, select **Tools and settings** and then select **Manage apps**.



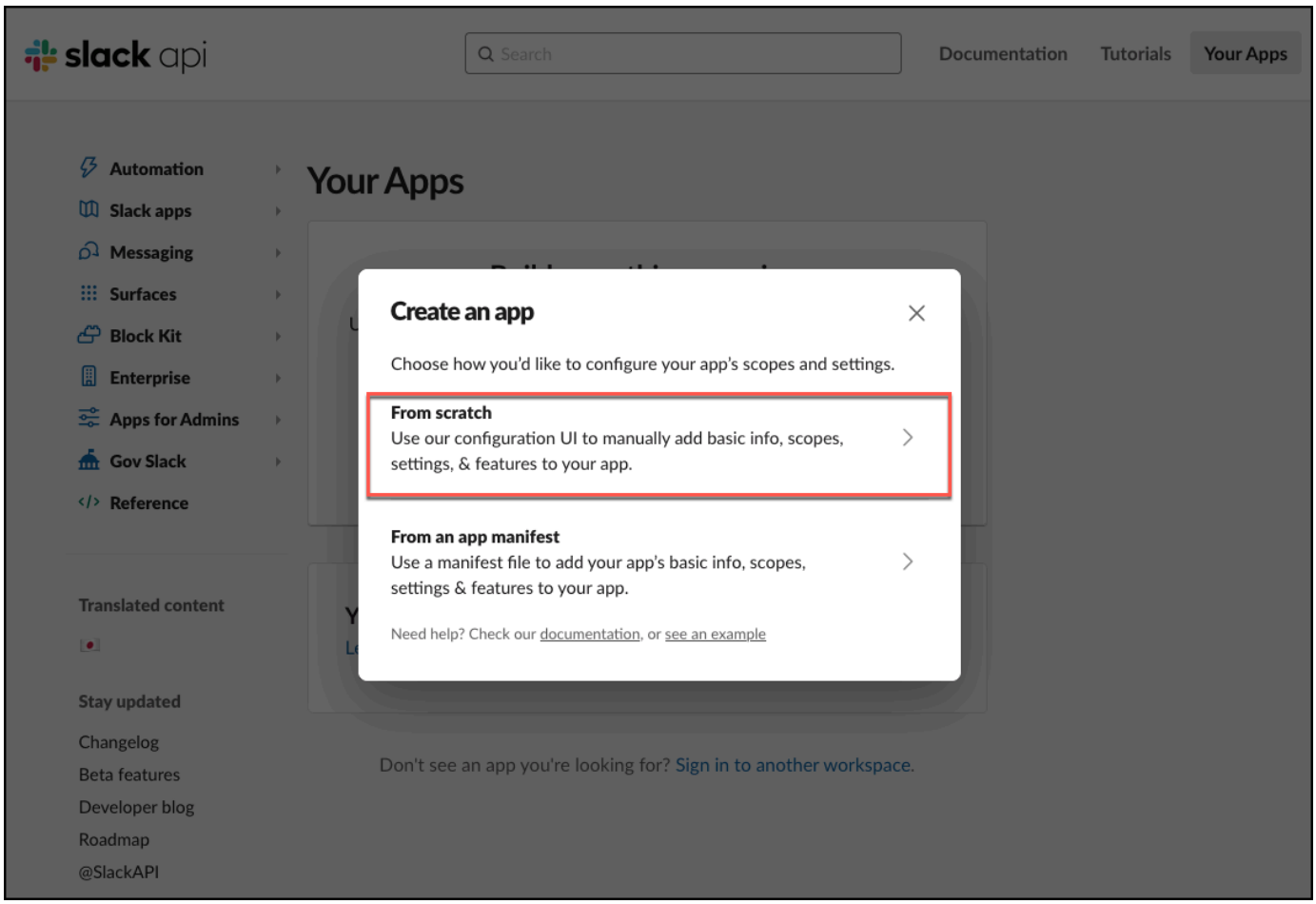
3. From the **Slack App Directory** menu, select **Build**.



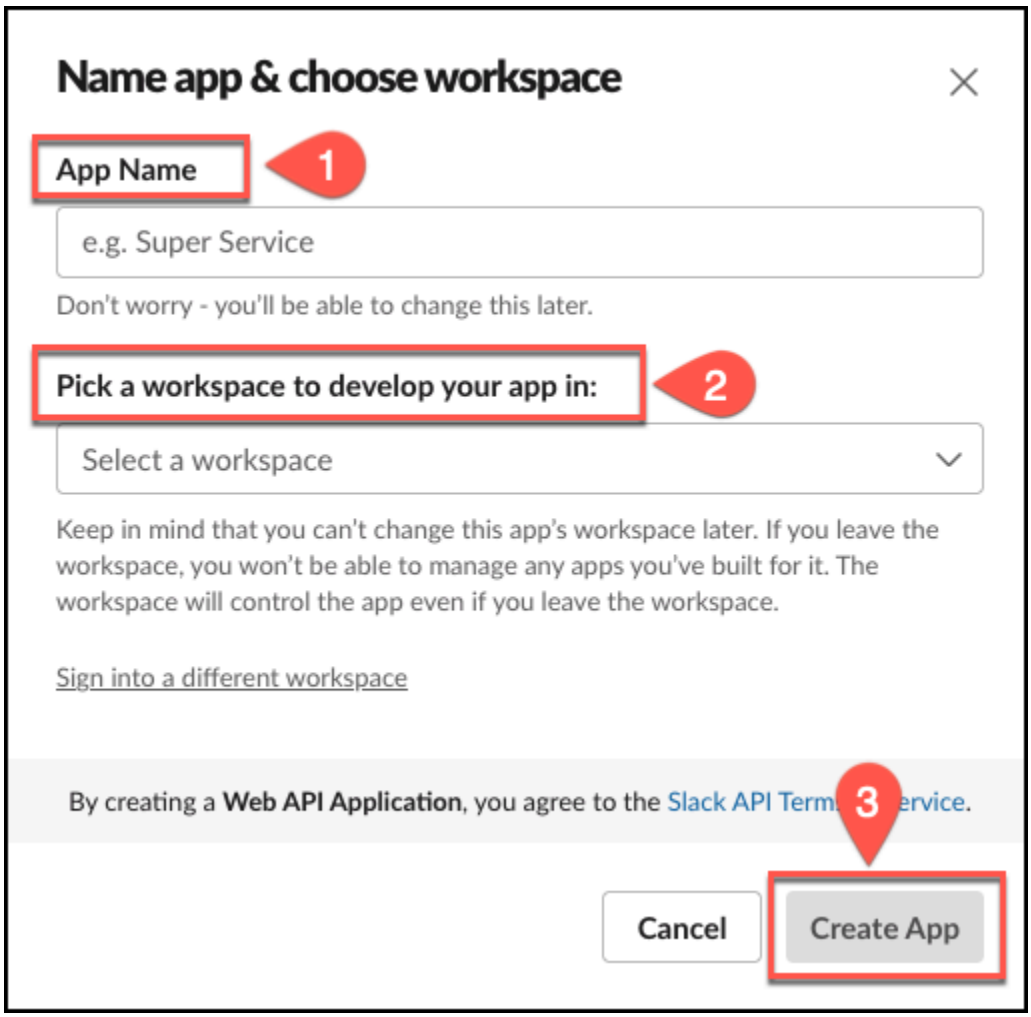
4. On the **Your Apps** page, select **Create an App**.



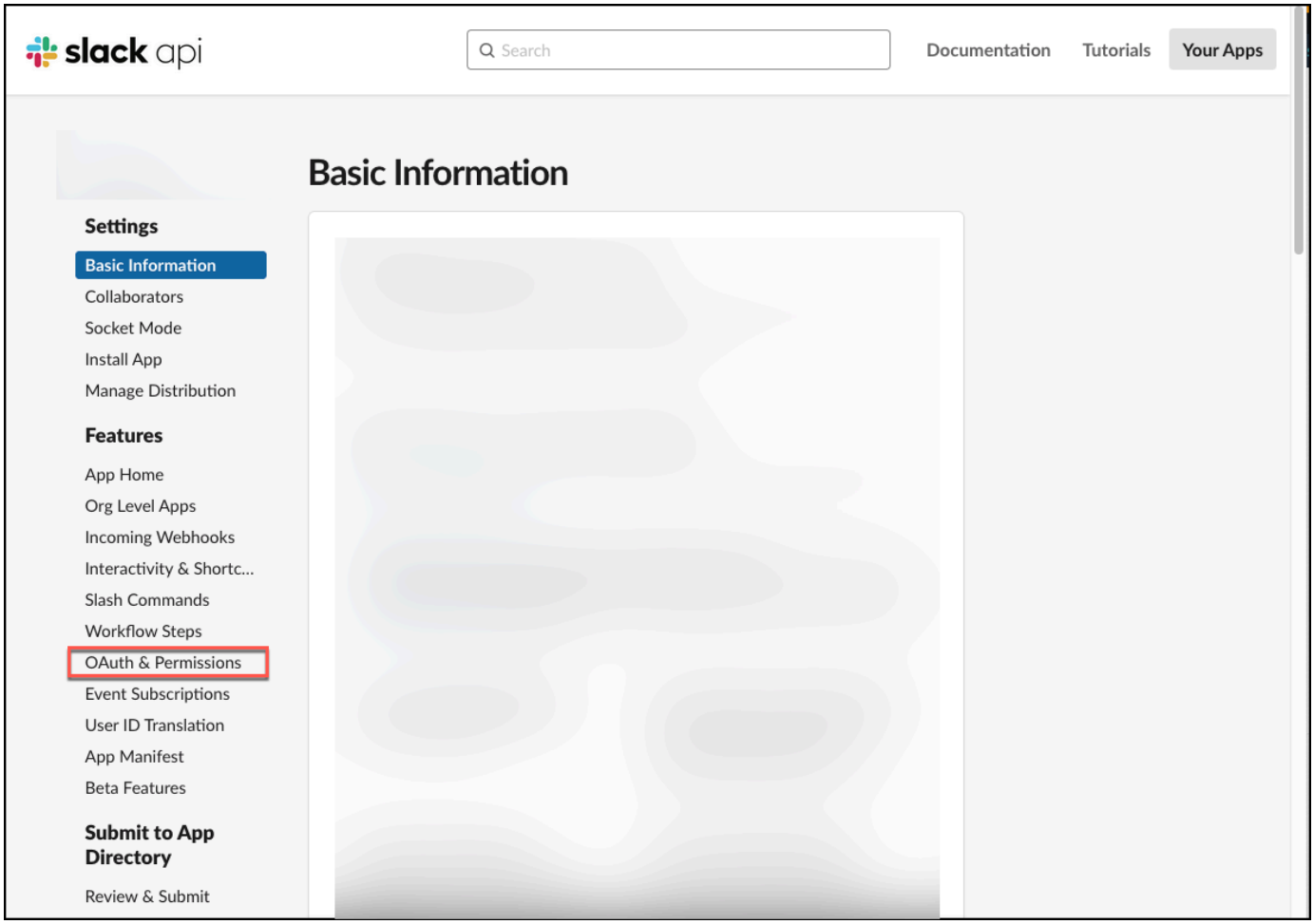
5. On the **Create an app** page, select **From scratch**.



6. In the **Name app & choose workspace** dialog box that opens, add an **App name** and **Pick a workspace to deploy your app in**. Then select **Create App**.



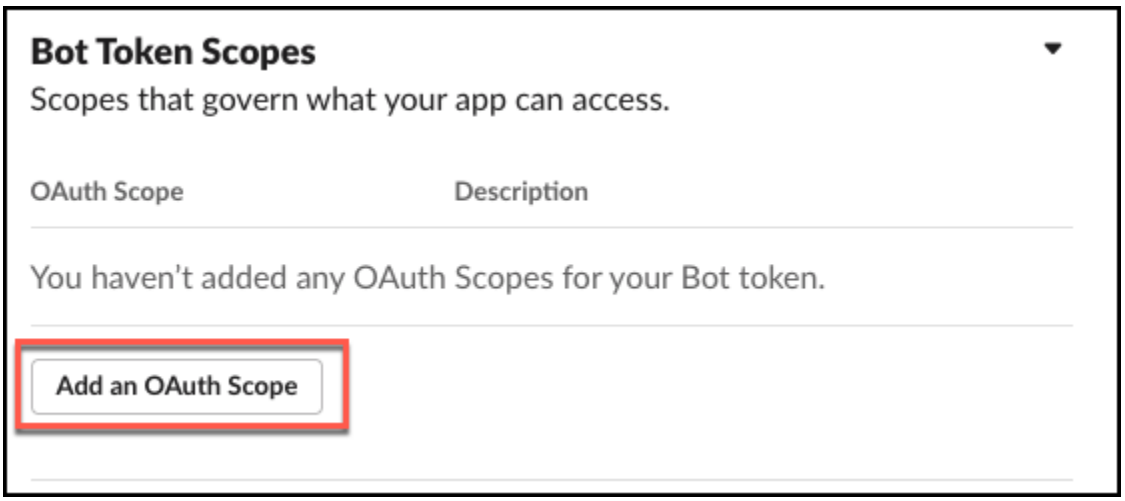
7. On the **Basic Information** page, from the **Settings** menu, select **OAuth & Permissions**.



8. On the **OAuth & Permissions** page, go to **Scopes**, and then do the following based on whether you want to use a Bot Token to connect Slack to Amazon Q, or a User Token:

> **Important**
>
> If you use the bot token as part of your Slack credentials, you cannot index direct messages and group messages, and you must add the bot token to the channel you want to index. For information on Slack token types, see Token types in Slack API.

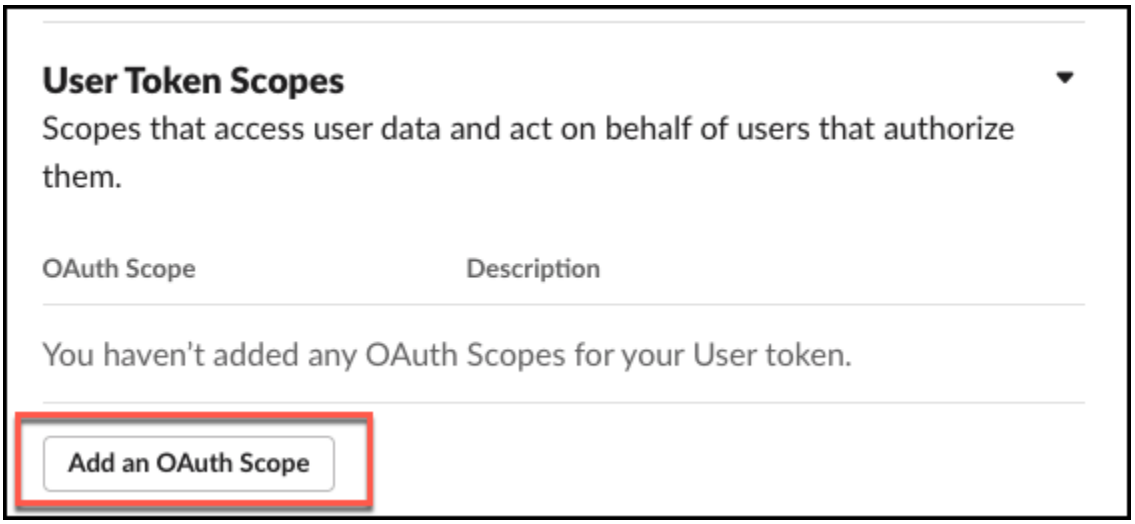
- Add the following **Bot Token Scopes**:



- `channels:history` – View messages and other content in public channels that your app has been added to
- `channels:manage` – Manage public channels that your app has been added to and create new ones
- `channels:read` – View basic information about public channels in a workspace
- `conversations.connect:manage` – Receive Slack Connect invite events sent to the channels your app is in
- `conversations.connect:read` – Receive Slack Connect invite events sent to the channels your app is in
- `files:read` – View files shared in channels and conversations that your app has been added to
- `groups:history` – View messages and other content in private channels that your app has been added to
- `groups:read` – View basic information about private channels that your app has been added to
- `im:history` – View messages and other content in direct messages that your app has been added to
- `im:read` – View basic information about direct messages that your app has been added to
- `mpim:history` – View messages and other content in group direct messages that your app has been added to
- `mpim:read` – View basic information about group direct messages that your app has been added to

- `reactions:read` – View emoji reactions and their associated content in channels and conversations that your app has been added to
- `team:read` – View the name, email domain, and icon for workspaces your app is connected to
- `usergroups:read` – Create and manage user groups
- `users.profile:read` – View profile details about people in a workspace
- `users:read` – View people in a workspace
- `users:read.email` – View email addresses of people in a workspace

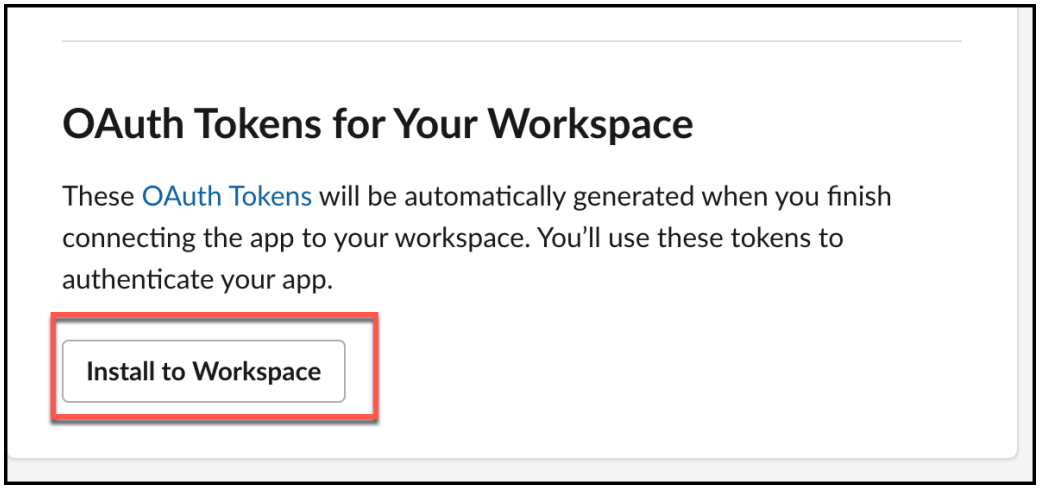
- Add the following **User Token Scopes**:



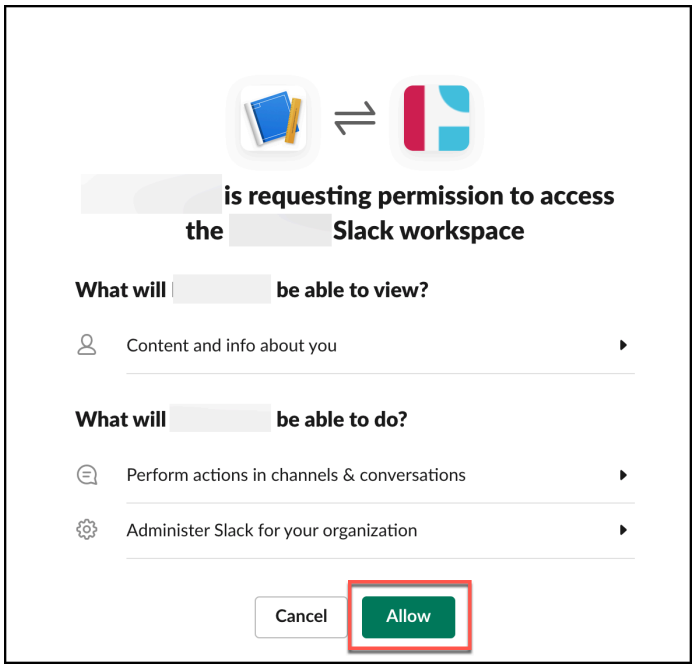
- `channels:history` – View messages and other content in a user's public channels
- `channels:read` – View basic information about public channels in a workspace
- `emoji:read` – View custom emoji in a workspace
- `files:read` – View files shared in channels and conversations that a user has access to
- `groups:history` – View messages and other content in a user's private channels
- `groups:read` – View basic information about a user's private channels
- `im:history` – View messages and other content in a user's direct messages
- `im:read` – View basic information about a user's direct messages
- `mpim:history` – View messages and other content in a user's group direct messages
- `mpim:read` – View basic information about a user's group direct messages
- `team:read` – View the name, email domain, and icon for workspaces a user is connected to

- `users.profile:read` – View profile details about people in a workspace
- `users:read.email` – View email addresses of people in a workspace
- `users:read` – View people in a workspace

9. Then, scroll to **OAuth Tokens** section, and choose **Install to Workspace**.

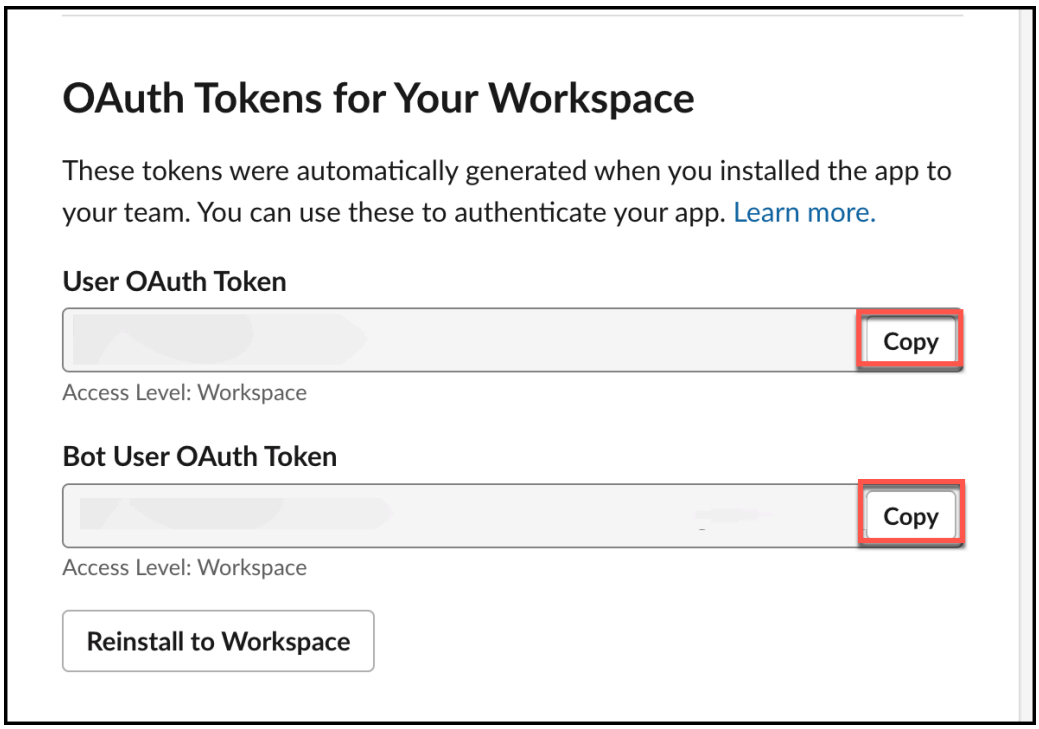


10. On the dialog box that opens up informing you that the app that you created is requesting permission to access the Slack workspace you wanted to connect it to, select **Allow**.



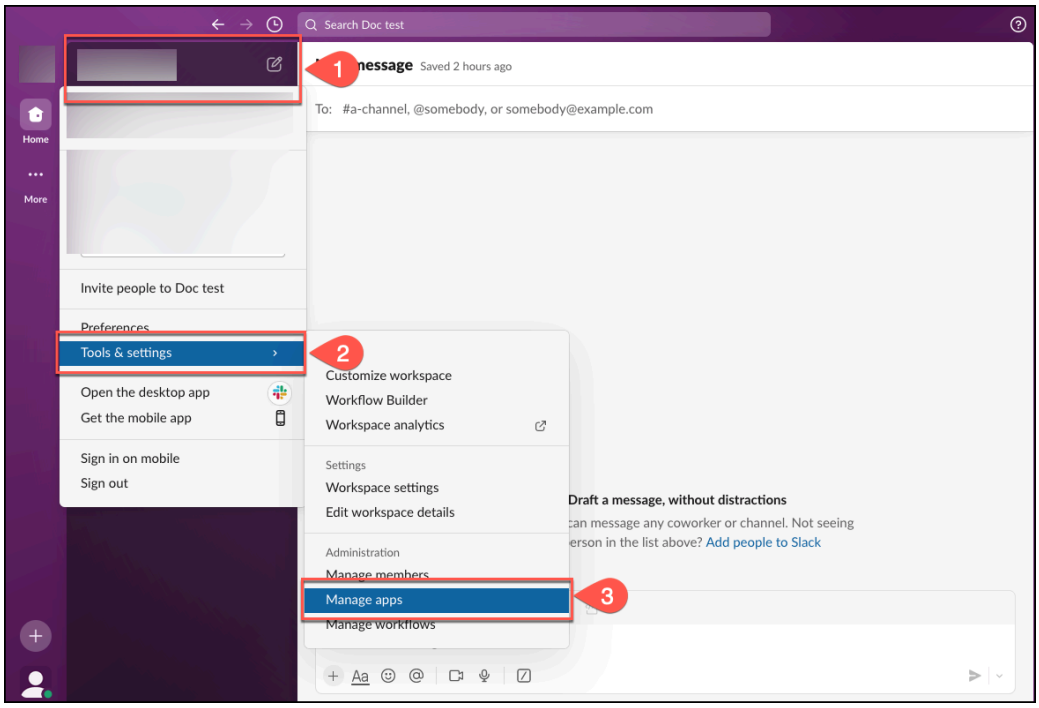
On successful completion, the console will display a **OAuth Tokens** screen.

11. From the **OAuth Tokens** screen, copy and save the OAuth token you will use to connect to Amazon Q—either **User OAuth Token** or **Bot User OAuth Token**. You input this as **Slack token** when you connect to Amazon Q.



12. Next, you retrieve your Slack team ID. You need this to connect to Amazon Q.

    From the Slack workspace menu, select **Tools and settings** and then select **Manage apps**. You'll find your team ID in the URL of the page that opens.



You now have the Slack Team ID and Slack token you need to connect to Amazon Q.

Connecting Amazon Q Business to Slack using the console

The following procedure outlines how to connect Amazon Q Business to Slack using the AWS Management Console.

Connecting Amazon Q to Slack

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Slack** data source to your Amazon Q application.
5. Then, on the **Slack** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **Source**, **Slack workspace team ID** – The team ID of your Slack workspace.
8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
9. **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

   b. For **Slack token** – Enter the authentication credential values you created in your Slack account.

10. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

    a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

    b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

    For more information, see VPC.

11. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

    > **Note**
    >
    > Creating a new service IAM role is recommended.

    For more information, see IAM role.

12. In **Sync scope**, enter the following information:

    a. **Select type of content to crawl** – Select any combination of **All channels**, **Public channels**, **Private channels**, **Group messages**, and **Private messages**.

    b. **Select crawl start date** – Choose the date from which the Amazon Q connector will start crawling content.

    c. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

    d. **Additional configuration – optional** – Configure the following settings:

    - In **Channels** (available only if you've chosen to crawl **Channels**), do the following:
      - **Channel ID/Name** – Choose between **Channel ID** and **Channel Name**.

        > **Note**
        >
        > You can choose to configure both.

- For **Channel ID** – Enter the **Channel ID**. The **Channel ID** filter applies to both public and private channels.
- For **Channel Name** – Choose the **Channel type** and enter the **Channel name**. You can select between **Public channel** and **Private channel**.

> **Note**
>
> If you choose to configure filters for both **Channel ID** and **Channel Name**, the Amazon Q Slack connector will prioritize channel IDs over channel names.
> If you choose to configure filters for either **Channel ID** or **Channel Name**, the Amazon Q Slack connector will ignore **Private** and **Group** messages even if you've chosen to crawl private and group messages in **Sync scope**.

- In **Messages**, for **Select sync scope for content** – Choose to **Include bot messages**, and/or **Include archived messaged**.
- **Regex patterns** – Add regex patterns to include or exclude file names or file types. You can add a total of 100 patterns. Examples of regex patterns include:
  - **File type** – .pdf, .docx
  - **File name** – Hello*.txt, TestFile.*

e. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

To extract audio transcriptions and video content, enable processing for the following file types:

f. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

13. For **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

- **Full sync**—Sync all content regardless of the previous sync status.

- **New, modified, or deleted content sync**—Sync only new, modified, and deleted documents.

14. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
15. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
16. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

17. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.

You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Slack using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

Topics

- Slack configuration properties
- Slack JSON schema
- Slack JSON schema example

Slack configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has the following sub-property: `repositoryEndpointMetadata` .	Yes

Configuration	Description	Type	Required
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-property: `teamId`.	Yes
`teamId`	The Slack team ID you copied from your Slack main page URL.	`string`	Yes
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object` This property has the following sub-property: `All`.	No
`All`	A list of objects that map the attributes or field names of your Slack pages and assets to Amazon Q index field names.	`object` This property has the following sub-properties: `indexFieldName`, `indexFieldType`, `dataSourceFieldName`, and `dateFieldFormat`.	Yes
`indexFieldName`	The field name of your Slack pages and assets.	`string`	Yes

Configuration	Description	Type	Required
`indexFieldType`	The field type of your Slack pages and assets.	`string` The allowed values are `STRING`, `STRING_LIST` , and `DATE`.	Yes
`dataSourceFieldName`	The data source field name of your Slack pages and assets.	`string`	Yes
`dateFieldFormat`	The date format of your Slack pages and assets.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties. • isCrawlAcl • conversationType • crawlBotMessages • excludeArchived • sinceDate • lookBack • fieldForUserId • maxFileSizeInMegaBytes • channelFilter • channelIdFilter • exclusionPatterns • inclusionPatterns	Yes

Configuration	Description	Type	Required
`isCrawlAcl`	Specify `true` to crawl access control information from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.	`boolean`	No

Configuration	Description	Type	Required
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string`	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No

Configuration	Description	Type	Required
`inclusionPatterns`	A list of regular expression patterns to include specific content in your Slack data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array`	No

Configuration	Description	Type	Required
`exclusionPatterns`	A list of regular expression patterns to exclude specific content in your Slack data source. Content that matches the patterns are excluded from the index. Content that doesn't match the patterns are included in the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array`	No
`crawlBotMessages`	`true` to crawl Slack bot messages.	`boolean`	No
`excludeArchived`	`true` to exclude archived messages from crawl.	`boolean`	No
`conversationType`	The type of conversation that you want to index.	`string` Valid values are `PUBLIC_CHANNEL`, `PRIVATE_CHANNEL`, `GROUP_MESSAGE`, and `DIRECT_MESSAGE`.	No

Configuration	Description	Type	Required
channelFilter	The type of channel that you want to index whether private_channel or public_channel .	object This property has the following sub-properties: private_channel and public_channel .	No
private_channel	The IDs of the private channel that you want to index.	array	No
public_channel	The IDs of public channel that you want to index.	array	No
channelIdFilter	You can choose to crawl specific channels vy channel ID using the channelIdFilter .	array	No
sinceDate	You can choose to configure a sinceDate parameter so that the Slack connector crawls content based on a specific sinceDate .	string Specify the date in the form ^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$ or as an empty string.	No

Configuration	Description	Type	Required
`lookBack`	You can choose to configure a `lookBack` parameter so that the Slack connector crawls `lookBack` content.	`string` Specify the value in the form `^[0-9]*$`.	No

Configuration	Description	Type	Required
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	`string` You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes
`type`	The type of data source. Specify SLACK as your data source type.	`string`	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/principal information on users and groups with access to specific documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.	`boolean`	Yes

Configuration	Description	Type	Required

`secretArn`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Slack.	`string`
		
		The secret must contain a JSON structure with the following keys:
		
		`{ "slackToken": " token" }`
			Yes

`version`	The version of this template that's currently supported.	`string`	No

Slack JSON schema

The following is the Slack JSON schema:

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "pattern": "SLACK"
    },
    "syncMode": {
      "type": "string",
      "enum": ["FORCED_FULL_CRAWL", "FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string"
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
```

```
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "teamId": {
              "type": "string"
            }
          },
          "required": ["teamId"]
        }
      }
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "All": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
```

```
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    },
    "required": []
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "isCrawlAcl": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
      },
      "fieldForUserId": {
        "type": "string"
      },
      "exclusionPatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
```

```
        "inclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "crawlBotMessages": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "excludeArchived": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "conversationType": {
          "type": "array",
          "items": {
            "type": "string",
            "enum": [
              "PUBLIC_CHANNEL",
              "PRIVATE_CHANNEL",
              "GROUP_MESSAGE",
              "DIRECT_MESSAGE"
            ]
          }
        },
        "channelFilter": {
          "type": "object",
          "properties": {
            "private_channel": {
```

```
            "type": "array",
            "items": {
              "type": "string"
            }
          },
          "public_channel": {
            "type": "array",
            "items": {
              "type": "string"
            }
          }
        }
      },
      "channelIdFilter": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "sinceDate": {
        "anyOf": [
          {
            "type": "string",
            "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
          },
          {
            "type": "string",
            "pattern": ""
          }
        ]
      },
      "lookBack": {
        "type": "string",
        "pattern": "^[0-9]*$"
      },
      "enableDeletionProtection": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
```

```
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    },
    "required": [
      "type",
      "secretArn",
      "syncMode",
      "enableIdentityCrawler",
      "connectionConfiguration",
      "repositoryConfigurations",
      "additionalProperties"
    ]
  }
}
```

Slack JSON schema example

The following is the Slack JSON schema example:

```
{
  "type": "SLACK",
  "syncMode": "FULL_CRAWL",
  "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-slack-secret",
  "enableIdentityCrawler": "true",
  "connectionConfiguration": {
    "repositoryEndpointMetadata": {
      "teamId": "T12345678"
    }
  },
```

```
  "repositoryConfigurations": {
    "All": {
      "fieldMappings": [
        {
          "indexFieldName": "message_id",
          "indexFieldType": "STRING",
          "dataSourceFieldName": "id",
          "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ]
    }
  },
  "additionalProperties": {
    "isCrawlAcl": "true",
    "maxFileSizeInMegaBytes": "50",
    "fieldForUserId": "user_id",
    "exclusionPatterns": ["*.tmp"],
    "inclusionPatterns": ["*"],
    "crawlBotMessages": "false",
    "excludeArchived": "true",
    "conversationType": ["PUBLIC_CHANNEL", "PRIVATE_CHANNEL"],
    "channelFilter": {
      "private_channel": ["C12345678"],
      "public_channel": ["C87654321"]
    },
    "channelIdFilter": ["C12345678"],
    "sinceDate": "2023-01-01T00:00:00Z",
    "lookBack": "7",
    "enableDeletionProtection": "false",
    "deletionProtectionThreshold": "15"
  },
  "version": "1.0.0"
}
```

Connecting Amazon Q Business to Slack using AWS CloudFormation

You use the `AWS::QBusiness::DataSource` resource to connect a data source to your Amazon Q application.

Use the `configuration` property to provide a JSON or YAML schema with the necessary configuration details specific to your data source connector.

To learn more about AWS CloudFormation, see What is AWS CloudFormation? in the *CloudFormation User Guide*.

Topics

- Slack configuration properties
- Slack JSON schema for using the configuration property with AWS CloudFormation
- Slack YAML schema for using the configuration property with AWS CloudFormation

Slack configuration properties

The following provides information about important configuration properties required in the schema.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration information for the endpoint for the data source.	`object` This property has the following sub-property: `repositoryEndpointMetadata` .	Yes
`repositoryEndpointMetadata`	The endpoint information for the data source.	`object` This property has the following sub-property: `teamId`.	Yes
`teamId`	The Slack team ID you copied from your Slack main page URL.	`string`	Yes
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific	`object` This property has the following sub-property: `All`.	No

Configuration	Description	Type	Required
	types of content and field mappings.		
`All`	A list of objects that map the attributes or field names of your Slack pages and assets to Amazon Q index field names.	`object` This property has the following sub-properties: `indexFieldName`, `indexFieldType`, `dataSourceFieldName`, and `dateFieldFormat`.	Yes
`indexFieldName`	The field name of your Slack pages and assets.	`string`	Yes
`indexFieldType`	The field type of your Slack pages and assets.	`string` The allowed values are `STRING`, `STRING_LIST`, and `DATE`.	Yes
`dataSourceFieldName`	The data source field name of your Slack pages and assets.	`string`	Yes
`dateFieldFormat`	The date format of your Slack pages and assets.	`string` Specify the date format in the form `yyyy-MM-dd'T'HH:mm:ss'Z'`	No

Configuration	Description	Type	Required
additionalProperties	Additional configuration options for your content in your data source.	object This property has the following sub-properties. • isCrawlAcl • conversationType • crawlBotMessages • excludeArchived • sinceDate • lookBack • fieldForUserId • maxFileSizeInMegaBytes • channelFilter • channelIdFilter • exclusionPatterns • inclusionPatterns	Yes

Configuration	Description	Type	Required
`isCrawlAcl`	Specify `true` to crawl access control information from documents. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.	`boolean`	No

Configuration	Description	Type	Required
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.	`string`	No
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.	`string`	No

Configuration	Description	Type	Required
`inclusionPatterns`	A list of regular expression patterns to include specific content in your Slack data source. Content that matches the patterns are included in the index. Content that doesn't match the patterns are excluded from the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array`	No

Configuration	Description	Type	Required
`exclusionPatterns`	A list of regular expression patterns to exclude specific content in your Slack data source. Content that matches the patterns are excluded from the index. Content that doesn't match the patterns are included in the index. If any content matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the content isn't included in the index.	`array`	No
`crawlBotMessages`	`true` to crawl Slack bot messages.	`boolean`	No
`excludeArchived`	`true` to exclude archived messages from crawl.	`boolean`	No
`conversationType`	The type of conversation that you want to index.	`string` Valid values are `PUBLIC_CHANNEL`, `PRIVATE_CHANNEL`, `GROUP_MESSAGE`, and `DIRECT_MESSAGE`.	No

Configuration	Description	Type	Required
`channelFilter`	The type of channel that you want to index whether `private_channel` or `public_channel` .	`object` This property has the following sub-properties: `private_channel` and `public_channel` .	No
`private_channel`	The IDs of the private channel that you want to index.	`array`	No
`public_channel`	The IDs of public channel that you want to index.	`array`	No
`channelIdFilter`	You can choose to crawl specific channels vy channel ID using the `channelIdFilter` .	`array`	No
`sinceDate`	You can choose to configure a `sinceDate` parameter so that the Slack connector crawls content based on a specific `sinceDate` .	`string` Specify the date in the form `^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$` or as an empty string.	No

Configuration	Description	Type	Required
`lookBack`	You can choose to configure a `lookBack` parameter so that the Slack connector crawls `lookBack` content.	`string` Specify the value in the form `^[0-9]*$`.	No

Configuration	Description	Type	Required
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	`string` You can choose between the following options: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes
`type`	The type of data source. Specify SLACK as your data source type.	`string`	Yes

Configuration	Description	Type	Required
`enableIdentityCrawler`	Specify `true` to use the Amazon Q identity crawler to sync identity/principal information on users and groups with access to specific documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.	`boolean`	Yes

Configuration	Description	Type	Required

`secretArn`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Slack.	`string`
		
		The secret must contain a JSON structure with the following keys:
		
		`{ "slackToken": " token" }`
			Yes

`version`	The version of this template that's currently supported.	`string`	No

Slack JSON schema for using the configuration property with AWS CloudFormation

The following is the Slack JSON schema and examples for the configuration property for AWS CloudFormation.

Topics

- Slack JSON schema for using the configuration property with AWS CloudFormation
- Slack JSON schema example for using the configuration property with AWS CloudFormation

Slack JSON schema for using the configuration property with AWS CloudFormation

The following is the Slack JSON schema for the configuration property for CloudFormation

```
{
  "type": "object",
  "properties": {
    "type": {
      "type": "string",
      "pattern": "SLACK"
    },
    "syncMode": {
```

```
      "type": "string",
      "enum": ["FORCED_FULL_CRAWL", "FULL_CRAWL", "CHANGE_LOG"]
    },
    "secretArn": {
      "type": "string"
    },
    "enableIdentityCrawler": {
      "anyOf": [
        {
          "type": "boolean"
        },
        {
          "type": "string",
          "enum": ["true", "false"]
        }
      ]
    },
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "teamId": {
              "type": "string"
            }
          },
          "required": ["teamId"]
        }
      }
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "All": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
```

```
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    },
    "required": []
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "isCrawlAcl": {
        "anyOf": [
          {
            "type": "boolean"
          },
          {
            "type": "string",
            "enum": ["true", "false"]
          }
        ]
      },
      "maxFileSizeInMegaBytes": {
        "type": "string"
```

```
        },
        "fieldForUserId": {
          "type": "string"
        },
        "exclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionPatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "crawlBotMessages": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "excludeArchived": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ]
        },
        "conversationType": {
          "type": "array",
          "items": {
            "type": "string",
            "enum": [
              "PUBLIC_CHANNEL",
```

```
            "PRIVATE_CHANNEL",
            "GROUP_MESSAGE",
            "DIRECT_MESSAGE"
          ]
        }
      },
      "channelFilter": {
        "type": "object",
        "properties": {
          "private_channel": {
            "type": "array",
            "items": {
              "type": "string"
            }
          },
          "public_channel": {
            "type": "array",
            "items": {
              "type": "string"
            }
          }
        }
      },
      "channelIdFilter": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "sinceDate": {
        "anyOf": [
          {
            "type": "string",
            "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
          },
          {
            "type": "string",
            "pattern": ""
          }
        ]
      },
      "lookBack": {
        "type": "string",
        "pattern": "^[0-9]*$"
```

```
        },
        "enableDeletionProtection": {
          "anyOf": [
            {
              "type": "boolean"
            },
            {
              "type": "string",
              "enum": ["true", "false"]
            }
          ],
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
      },
      "required": []
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    },
    "required": [
      "type",
      "secretArn",
      "syncMode",
      "enableIdentityCrawler",
      "connectionConfiguration",
      "repositoryConfigurations",
      "additionalProperties"
    ]
  }
}
```

Slack JSON schema example for using the configuration property with AWS CloudFormation

The following is the Slack JSON schema example for the configuration property for CloudFormation

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "CloudFormation SLACK Data Source Template",
  "Resources": {
    "DataSourceSlack": {
      "Type": "AWS::QBusiness::DataSource",
      "Properties": {
        "ApplicationId": "app12345-1234-1234-1234-123456789012",
        "IndexId": "indx1234-1234-1234-1234-123456789012",
        "DisplayName": "MySlackDataSource",
        "RoleArn": "arn:aws:iam::123456789012:role/qbusiness-data-source-role",
        "Configuration": {
          "type": "SLACK",
          "syncMode": "FULL_CRAWL",
          "secretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:my-slack-
secret",
          "enableIdentityCrawler": "true",
          "connectionConfiguration": {
            "repositoryEndpointMetadata": {
              "teamId": "T12345678"
            }
          },
          "repositoryConfigurations": {
            "All": {
              "fieldMappings": [
                {
                  "indexFieldName": "message_id",
                  "indexFieldType": "STRING",
                  "dataSourceFieldName": "id",
                  "dateFieldFormat": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              ]
            }
          },
          "additionalProperties": {
            "isCrawlAcl": "true",
            "maxFileSizeInMegaBytes": "50",
            "fieldForUserId": "user_id",
            "exclusionPatterns": ["*.tmp"],
```

```
            "inclusionPatterns": ["*"],
            "crawlBotMessages": "false",
            "excludeArchived": "true",
            "conversationType": ["PUBLIC_CHANNEL", "PRIVATE_CHANNEL"],
            "channelFilter": {
              "private_channel": ["C12345678"],
              "public_channel": ["C87654321"]
            },
            "channelIdFilter": ["C12345678"],
            "sinceDate": "2023-01-01T00:00:00Z",
            "lookBack": "7",
            "enableDeletionProtection": "false",
            "deletionProtectionThreshold": "15"
          }
        }
      }
    }
  }
}
```

Slack YAML schema for using the configuration property with AWS CloudFormation

The following is the Slack YAML schema and examples for the configuration property for AWS CloudFormation:

Topics

- Slack YAML schema for using the configuration property with AWS CloudFormation
- Slack YAML schema example for using the configuration property with AWS CloudFormation

Slack YAML schema for using the configuration property with AWS CloudFormation

The following is the Slack YAML schema for the configuration property for CloudFormation.

```
type: object
properties:
  type:
    type: string
    pattern: SLACK
  syncMode:
    type: string
    enum:
      - FORCED_FULL_CRAWL
```

```
      - FULL_CRAWL
      - CHANGE_LOG
  secretArn:
    type: string
  enableIdentityCrawler:
    anyOf:
      - type: boolean
      - type: string
        enum:
          - true
          - false
  connectionConfiguration:
    type: object
    properties:
      repositoryEndpointMetadata:
        type: object
        properties:
          teamId:
            type: string
        required:
          - teamId
  repositoryConfigurations:
    type: object
    properties:
      All:
        type: object
        properties:
          fieldMappings:
            type: array
            items:
              type: object
              properties:
                indexFieldName:
                  type: string
                indexFieldType:
                  type: string
                  enum:
                    - STRING
                    - STRING_LIST
                    - DATE
                    - LONG
                dataSourceFieldName:
                  type: string
                dateFieldFormat:
```

```
                type: string
                pattern: "yyyy-MM-dd'T'HH:mm:ss'Z'"
            required:
              - indexFieldName
              - indexFieldType
              - dataSourceFieldName
      required:
        - fieldMappings
  additionalProperties:
    type: object
    properties:
      isCrawlAcl:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      maxFileSizeInMegaBytes:
        type: string
      fieldForUserId:
        type: string
      exclusionPatterns:
        type: array
        items:
          type: string
      inclusionPatterns:
        type: array
        items:
          type: string
      crawlBotMessages:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
      excludeArchived:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
```

```
      conversationType:
        type: array
        items:
          type: string
          enum:
            - PUBLIC_CHANNEL
            - PRIVATE_CHANNEL
            - GROUP_MESSAGE
            - DIRECT_MESSAGE
      channelFilter:
        type: object
        properties:
          private_channel:
            type: array
            items:
              type: string
          public_channel:
            type: array
            items:
              type: string
      channelIdFilter:
        type: array
        items:
          type: string
      sinceDate:
        anyOf:
          - type: string
            pattern: "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
          - type: string
            pattern: ""
      lookBack:
        type: string
        pattern: "^[0-9]*$"
      enableDeletionProtection:
        anyOf:
          - type: boolean
          - type: string
            enum:
              - true
              - false
        default: false
      deletionProtectionThreshold:
        type: string
        default: "15"
```

```
    required: []
  version:
    type: string
    anyOf:
      - pattern: 1.0.0
required:
  - type
  - secretArn
  - syncMode
  - enableIdentityCrawler
  - connectionConfiguration
  - repositoryConfigurations
  - additionalProperties
```

Slack YAML schema example for using the configuration property with AWS CloudFormation

The following is the Slack YAML example for the Configuration property for CloudFormation:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: CloudFormation SLACK Data Source Template
Resources:
  DataSourceSlack:
    Type: AWS::QBusiness::DataSource
    Properties:
      ApplicationId: app12345-1234-1234-1234-123456789012
      IndexId: indx1234-1234-1234-1234-123456789012
      DisplayName: MySlackDataSource
      RoleArn: arn:aws:iam::123456789012:role/qbusiness-data-source-role
      Configuration:
        type: SLACK
        syncMode: FULL_CRAWL
        secretArn: arn:aws:secretsmanager:us-west-2:123456789012:secret:my-slack-secret
        enableIdentityCrawler: "true"
        connectionConfiguration:
          repositoryEndpointMetadata:
            teamId: T12345678
        repositoryConfigurations:
          All:
            fieldMappings:
              - indexFieldName: message_id
                indexFieldType: STRING
                dataSourceFieldName: id
                dateFieldFormat: yyyy-MM-dd'T'HH:mm:ss'Z'
        additionalProperties:
```

```
          isCrawlAcl: "true"
          maxFileSizeInMegaBytes: "50"
          fieldForUserId: user_id
          exclusionPatterns:
            - "*.tmp"
          inclusionPatterns:
            - "*"
          crawlBotMessages: "false"
          excludeArchived: "true"
          conversationType:
            - PUBLIC_CHANNEL
            - PRIVATE_CHANNEL
          channelFilter:
            private_channel:
              - C12345678
            public_channel:
              - C87654321
          channelIdFilter:
            - C12345678
          sinceDate: "2023-01-01T00:00:00Z"
          lookBack: "7"
          enableDeletionProtection: "false"
          deletionProtectionThreshold: "15"
```

How Amazon Q Business connector crawls Slack ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

Slack organizes content into documents, which include messages, attachments, posts, snippets, thread replies, and emojis. Messages and attachments can belong to different conversation types such as direct messages (DMs), public channels, or private channels.

When you connect a Slack data source to Amazon Q Business, Amazon Q Business crawls ACL information (channel IDs) attached to a document from your Slack instance. If you choose to activate ACL crawling, this information can be used to filter chat responses to your end user's document access level. Access Control (ACLs) in Slack is managed through users and groups.

Identity Crawling: Slack allows link sharing at the document level. If a document link is shared across different channels (DMs, groups, or private channels), the new channel ID is included during

crawling, effectively expanding ACLs to include members of those channels. Slack does not enforce explicit deny rules: public channels allow user removal but do not prevent them from rejoining, whereas private channels restrict reentry without an invitation. The minimum permission to query channel data varies: for public channels, workspace membership is sufficient, while private channels require direct membership for access. Slack enforces username restrictions, supporting only lowercase letters, numbers, periods, hyphens, and underscores. This lowercase format is maintained when crawling identities. ACL mismatches can occur if case differences exist between Slack usernames and identity data stored in the connector, potentially preventing access to crawled information. When a user is deactivated or deleted, they lose access to crawled data, and subsequent syncs reflect this by removing the user from ACLs.

Permission Inheritance: The Slack Workspace is the top-most entity controlling access. All workspace members can access public channels by default. Public channels have no ACLs; they are accessible to all workspace members. If ACLs are disabled, all public channel content is open to everyone on Amazon Q. DMs, groups, and private channels have independent ACLs, which completely replace any parent ACLs. Private channels restrict access to invited members, including external collaborators via Slack Connect. All entities inherit permissions from the parent.

Mapping Rules: Slack's inheritance mapping follows its native structure without custom logic. Federated groups are treated as local upon syncing, with all members stored regardless of status. Emails, links, and other text within messages are crawled as regular strings without specific parsing. Link-sharing does not modify document ACLs: a shared link in a message is crawled as plain text rather than as an access control change. Public channels are accessible to all Amazon Q users if no ACL is applied.

Failure handling: The connector follows a fail-close approach, meaning if there are permission-related issues or API failures, affected documents are skipped from ingestion rather than being made publicly accessible. This prevents unauthorized access while maintaining data integrity.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Slack data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Slack connector supports the following field mappings:

Slack field name	Index field name	Description	Data type
size	sl_gen_size	Custom	Long (numeric)
emojis	sl_gen_emojis	Custom	String list
title	sl_gen_title	Custom	String
authors	_authors	Default	String list

Slack field name	Index field name	Description	Data type
url	_source_uri	Default	String
category	sl_gen_category	Custom	String
created_at	_created_at	Default	Date
last_updated_at	_last_updated_at	Default	Date
msg_channel_id	sl_message_channel_id	Custom	String
msg_channel_name	sl_msg_channel_name	Custom	String

IAM role for the Slack connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
```

```
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
```

```
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Smartsheet to Amazon Q Business

Smartsheet is an enterprise work management platform that lets users manage projects, programs and processes at scale using sheets, channels, and workspaces. You can connect your Smartsheet instance to Amazon Q Business—using either the AWS Management Console, CLI, or the CreateDataSource API—and create an Amazon Q Business web experience.

Integrating Smartsheet as a data source in Amazon Q Business enables users to quickly get insights from project sheets. For example, users can ask questions like:

- "Which project manager is responsible for Project Harpo?", where the answer comes from a Smartsheet row
- "What are the requirements for the Create APIs task?", where the answer is fetched from a PDF attached to the row for Create APIs
- "Who is the owner of the Individual Task Management workspace?", where the answer comes from workspace metadata

With the Amazon Q Business Smartsheet connector, you can solve the following kinds of use cases.

- **Project status updates** – Get quick insights into project health without having to open Smartsheet with questions like:
  - "What's the status of the website redesign project?"
  - "Is the mobile app launch on track for the planned date?"
  - "Which projects are currently behind schedule in the Q3 Roadmap sheet?"
- **Task management** – Find information about tasks and action items with questions like:
  - "What tasks are assigned to Mary Major?"
  - "Has the marketing plan document been completed?"
  - "What's the due date for the customer research presentation?"

The Amazon Q Business Smartsheet connector understands user access permissions and strictly enforces them at the time of the query. This ensures that users aren't able to see content they don't have access to.

> **Note**
>
> We recommend enabling Cross-region inference for Amazon Q Business for your Amazon Q Business application connector to get the best customer experience with improved query response accuracy.

Topics

- Known limitations for the Smartsheet connector
- Prerequisites for connecting Amazon Q Business to Smartsheet
- Connecting Amazon Q Business to Smartsheet using the console

- Connecting Amazon Q Business to Smartsheet using APIs
- How Amazon Q Business connector crawls Smartsheet ACLs
- IAM role for Smartsheet connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Smartsheet connector

The Smartsheet connector has the following known limitations:

- If you remove users' access to a Smartsheet data source but not to Amazon Q Business, they will be able to receive responses from the data source when they query Amazon Q Business.
- The Smartsheet connector will provide responses from the most applicable single sheet. That is, it will search across all sheets and find the sheet with the most relevant answer and provide that instead of aggregating data across multiple sheets. For example, it can't answer questions like: "Show me tasks that are past due across all my sheets."
- For hierarchical sheets, Amazon Q Business accuracy can drop when queries are directly related to the hierarchical structure.

  For example, if a sheet has hierarchical structure about high-level tasks and its subtasks, and a user asks "What's the amount of time needed to finish all tasks?" then Amazon Q Business might add up all times assigned to both high-level tasks and the sub-tasks. This calculation is wrong as the amount of time to finish the high-level task is just a sum up of the sub-tasks.

  However, if the user asks a query such as "How many tasks are assigned to Mary Major?", they would get an accurate response.

- For sheets with similar names—(for example, “Blockchain Integration - Project Plan” and “Blockchain Integration - Impact Tracker”)—if a query mentions just “Blockchain Integration” then you might not get an accurate response. To get accurate responses, we recommend:
  - providing clearer titles/descriptions of the sheets, or
  - providing more detailed questions to reduce ambiguity.

Prerequisites for connecting Amazon Q Business to Smartsheet

Before you begin, make sure that you have completed the following prerequisites.

- **In Smartsheet, make sure you have:**
  - Access to the Smartsheet Event Reporting API. Use the Events API Access Request form to request access for your organization.
  - An Smartsheet system admin user or a licensed user for Smartsheet who can generate an access token. With this access token, your connector will have access to crawl all sheets and workspaces created by or shared with this user.
  - A Smartsheet access token. You need this to connect Smartsheet to Amazon Q Business. For information on how to generate this token in Smartsheet, see Authentication and Access Tokens in the *Smartsheet API Reference*.
- **In your AWS account, make sure you have:**
  - Created a Amazon Q Business application.
  - Created a Amazon Q Business retriever and added an index.
  - Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
  - Stored your Smartsheet authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you’re a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Connecting Amazon Q Business to Smartsheet using the console

The following procedure outlines how to connect Amazon Q Business to Smartsheet using the AWS Management Console.

> **Note**
>
> Before you begin adding your data source, make sure you've created an Amazon Q Business application, and added an index and retriever to it.

Connecting Amazon Q to Smartsheet

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Smartsheet** data source to your Amazon Q application.
5. Then, on the **Smartsheet** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

     > **Note**
     >
     > You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

   - **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.
7. In **User type** – Choose the user type in your Smartsheet account. You can choose between **System Admin** and **Non-System Admin**. System Admins can ingest sheets, folders, and workspaces into Amazon Q Business. Non-System Admins can ingest only sheets.
8. **Authentication** – Enter the following information for your **AWS Secrets Manager secret**.

   a. **Secret name** – A name for your secret.

b. For **Smartsheet API access token** – Enter the value for the access token you created in your Smartsheet account.

9. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

10. In **Sync scope**, enter the following information:

a. In **Select specific sheets, folders, and workspaces**, for **ID type** – Select content to sync using a specific **Sheet ID**, **Folder ID**, and **Workspace ID**.

b. For **Select attachments and conversations**, select from the following options:

- **All attachments** – Select to include all attachments.
- **All conversations** – Select to include all conversations.

c. In **Additional configuration – *optional*, select from the following options:**

- **Sheet and folder regex patterns** – Choose to include or exclude specific sheet and folder names using regex patterns.
- **Attachment regex patterns** – Choose to include or exclude specific files by name and type using regex patterns.

d. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.

e. **Multi-media content configuration – optional** – To enable content extraction from embedded images and visuals in documents, choose **Visual content in documents**.

To extract audio transcriptions and video content, enable processing for the following file types:

f. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

11. For **Sync mode**, choose how you want to update your index when your data source content changes. When you sync your data source with Amazon Q for the first time, all content is synced by default.

    - **Full sync**—Sync all content regardless of the previous sync status.
    - **New, modified, or deleted content sync**—Sync only new, modified, and deleted documents.

12. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule.

> **Note**
>
> The Amazon Q Business Smartsheet connector doesn't support hourly syncs. For optimal performance, choose to sync your data during a time window outside of 11am UTC to 11pm UTC.

13. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
14. **Field mappings** – A list of data source document attributes to map to your index fields. Add the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

    a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

    b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

15. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages, including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
> For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Smartsheet using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

JSON schema

The following is the Smartsheet JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
```

```
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "authType": {
              "type": "string",
              "enum": [
                "APIToken"
              ]
            }
          },
          "required": [
            "authType"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "sheet": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": [
                        "STRING",
                        "DATE",
                        "STRING_LIST",
                        "LONG"
                      ]
                    },
                    "dataSourceFieldName": {
```

```
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      },
      "sheetAttachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "DATE",
                      "STRING_LIST",
                      "LONG"
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
```

```
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "sheetConversation": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": [
                    "STRING",
                    "DATE",
                    "STRING_LIST",
                    "LONG"
                  ]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
```

```
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      },
      "sheetConversationAttachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "DATE",
                      "STRING_LIST",
                      "LONG"
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
```

```
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      },
      "rowAttachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "DATE",
                      "STRING_LIST",
                      "LONG"
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
```

```
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "rowConversation": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": [
                    "STRING",
                    "DATE",
                    "STRING_LIST",
                    "LONG"
                  ]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
```

```
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "rowConversationAttachment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": [
                    "STRING",
                    "DATE",
                    "STRING_LIST",
                    "LONG"
                  ]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
```

```
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "workspaceIds": {
        "type": "array",
        "items": {
          "type": "string"
        },
        "maxItems": 20
      },
      "sheetIds": {
        "type": "array",
        "items": {
          "type": "string"
        },
        "maxItems": 20
      },
      "folderIds": {
        "type": "array",
        "items": {
          "type": "string"
        },
        "maxItems": 20
      },
      "fieldForUserId": {
        "type": "string"
      },
      "userType": {
        "type": "string"
      },
      "isCrawlAcl": {
        "type": "boolean"
      },
      "isCrawlSheets": {
```

```
          "type": "boolean"
        },
        "isCrawlSheetAttachments": {
          "type": "boolean"
        },
        "isCrawlSheetConversations": {
          "type": "boolean"
        },
        "isCrawlSheetConversationAttachments": {
          "type": "boolean"
        },
        "isCrawlRows": {
          "type": "boolean"
        },
        "isCrawlRowAttachments": {
          "type": "boolean"
        },
        "isCrawlRowConversations": {
          "type": "boolean"
        },
        "isCrawlRowConversationAttachments": {
          "type": "boolean"
        },
        "isCrawlRowProofs": {
          "type": "boolean"
        },
        "isMetadataAppended": {
          "type": "boolean"
        },
        "isConversationAppended": {
          "type": "boolean"
        },
        "inclusionAttachmentTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionAttachmentTypePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
```

```
        "inclusionAttachmentNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionAttachmentNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionFolderNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionFolderNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "inclusionSheetNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionSheetNamePatterns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "enableDeletionProtection": {
          "type": "boolean",
          "default": false
        },
        "deletionProtectionThreshold": {
          "type": "string",
          "default": "15"
        }
```

```
      },
      "not": {
        "properties": {
          "workspaceIds": { "maxItems": 0 },
          "sheetIds": { "maxItems": 0 },
          "folderIds": { "maxItems": 0 }
        }
      }
    },
    "enableIdentityCrawler": {
      "type": "boolean"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FULL_CRAWL",
        "FORCED_FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "type": {
      "type": "string",
      "pattern": "SMARTSHEET"
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
```

```
    "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description	Type	Required
`connectionConfiguration`	Configuration details for connecting to the data source.	`object`	Yes
`connectionConfiguration.repositoryEndpointMetadata`	Metadata for the repository endpoint.	`object`	Yes
`connectionConfiguration.repositoryEndpointMetadata.authType`	The authentication type.	`string` The only allowed value is: • `APIToken`	Yes
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.	`object`	Yes
`repositoryConfigurations.sheet`	Configuration for Smartsheet sheets.	`object`	No

Configuration	Description	Type	Required
`repositoryConfigurations.sheet.fieldMappings`	Field mappings for Smartsheet sheets.	`array` of `object`	Yes (if sheet is present)
`repositoryConfigurations.sheetAttachment`	Configuration for Smartsheet sheet attachments.	`object`	No
`repositoryConfigurations.sheetConversation`	Configuration for Smartsheet sheet conversations.	`object`	No
`repositoryConfigurations.sheetConversationAttachment`	Configuration for Smartsheet sheet conversation attachments.	`object`	No
`repositoryConfigurations.row`	Configuration for Smartsheet rows.	`object`	No
`repositoryConfigurations.rowAttachment`	Configuration for row attachments.	`object`	No

Configuration	Description	Type	Required
repositoryConfigurations.rowConversation	Configuration for Smartsheet row conversations.	object	No
repositoryConfigurations.rowConversationAttachment	Configuration for Smartsheet row conversation attachments.	object	No
repositoryConfigurations.proofAttachment	Configuration for Smartsheet proof attachments.	object	No
repositoryConfigurations.proofConversation	Configuration for Smartsheet proof conversations.	object	No
repositoryConfigurations.proofConversationAttachment	Configuration for Smartsheet proof conversation attachments.	object	No
additionalProperties	Additional configuration options for your content in your data source.	object	Yes

Configuration	Description	Type	Required
additionalProperties.workspaceIds	List of Smartsheet workspace IDs to crawl.	array of string	No
additionalProperties.sheetIds	List of Smartsheet sheet IDs to crawl.	array of string	No
additionalProperties.folderIds	List of Smartsheet folder IDs to crawl.	array of string	No
additionalProperties.fieldForUserId	Field for user ID.	string	No
additionalProperties.userType	User type.	string	Yes
additionalProperties.isCrawlAcl	Whether to crawl ACL.	boolean	No
additionalProperties.isCrawlSheets	Whether to crawl Smartsheet sheets.	boolean	No
additionalProperties.isCrawlSheetAttachments	Whether to crawl Smartsheet sheet attachments.	boolean	No

Configuration	Description	Type	Required
additionalProperties.isCrawlSheetConversations	Whether to crawl Smartsheet sheet conversations.	boolean	No
additionalProperties.isCrawlSheetConversationAttachments	Whether to crawl Smartsheet sheet conversation attachments.	boolean	No
additionalProperties.isCrawlRows	Whether to crawl Smartsheet rows.	boolean	No
additionalProperties.isCrawlRowAttachments	Whether to crawl Smartsheet row attachments.	boolean	No
additionalProperties.isCrawlRowConversations	Whether to crawl Smartsheet row conversations.	boolean	No
additionalProperties.isCrawlRowConversationAttachments	Whether to crawl Smartsheet row conversation attachments.	boolean	No

Configuration	Description	Type	Required
additionalProperties.isCrawlRowProofs	Whether to crawl Smartsheet row proofs.	boolean	No
additionalProperties.isMetadataAppended	Whether to append Smartsheet metadata.	boolean	No
additionalProperties.isConversationAppended	Whether to append Smartsheet conversations.	boolean	No
additionalProperties.inclusionAttachmentTypePatterns	Patterns for including Smartsheet attachment types.	array of string	No
additionalProperties.exclusionAttachmentTypePatterns	Patterns for excluding Smartsheet attachment types.	array of string	No

Configuration	Description	Type	Required
additionalProperties.inclusionAttachmentNamePatterns	Patterns for including Smartsheet attachment names.	array of string	No
additionalProperties.exclusionAttachmentNamePatterns	Patterns for excluding Smartsheet attachment names.	array of string	No
additionalProperties.inclusionFolderNamePatterns	Patterns for including Smartsheet folder names.	array of string	No
additionalProperties.exclusionFolderNamePatterns	Patterns for excluding Smartsheet folder names.	array of string	No
additionalProperties.inclusionSheetNamePatterns	Patterns for including Smartsheet sheet names.	array of string	No

Configuration	Description	Type	Required
`additionalProperties.exclusionSheetNamePatterns`	Patterns for excluding Smartsheet sheet names.	`array` of `string`	No
`additionalProperties.enableDeletionProtection`	Whether to enable deletion protection. To learn more, see Document deletion safeguard.	`boolean`	No
`additionalProperties.deletionProtectionThreshold`	Threshold for deletion protection. To learn more, see Document deletion safeguard	`string`	No

Configuration	Description	Type	Required
`enableIdentityCrawler`	Whether to enable the identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to certain documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information,	`boolean`	No

Configuration	Description	Type	Required
	see Identity crawler.		
`syncMode`	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents.	`string` The allowed values are: • Use `FORCED_FULL_CRAWL` to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use `FULL_CRAWL` to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use `CHANGE_LOG` to incrementally crawl only new and modified content each time your data source syncs with your index.	Yes

Configuration	Description	Type	Required
`secretArn`	The ARN of the secret containing the Smartsheet credentials required to connect Amazon Q Business to Smartsheet.	`string` The minimum length is 20 and the maximum length is 2,048 characters.	Yes
`type`	The type of the data source.	`string` The only allowed value is: • `SMARTSHEET`	Yes
`version`	The version of the template that's currently supported.	`string` Must match the pattern "1.0.0".	No

How Amazon Q Business connector crawls Smartsheet ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

Smartsheet organizes its data into several entities, including Workspaces, Sheets, Rows, Columns, Attachments, and Comments. Workspaces serve as hierarchical containers that hold folders and individual sheets. Connectors support crawling ACL and identity information where applicable based on the data source. When you connect a Smartsheet data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your Smartsheet instance. The Smartsheet connector does not allow disabling ACLs, so you must always inforce permissions. ACL information can be used to filter chat responses based your end users' document access level.

Roles/Permissions: Users and groups can be assigned various roles including Admin, Editor, and Viewer. Permissions can be managed at different levels, including Workspaces, Sheets, and individual Rows. Smartsheet enforces an Allow Mode for ACLs, meaning permissions are granted explicitly without an explicit deny option. Sheets and Workspaces can be shared via links with different permission levels (View or Edit), but public link sharing is not supported. In addition, Smartsheet allows setting sheets as either searchable or non-searchable, and the connector ensures that this setting is honored when ingesting Smartsheet data. The minimum permission required to read a sheet or workspace is "Viewer". Proper mapping between Smartsheet ACLs and Amazon Q ACL definitions is essential to ensure security and permission consistency.

Identity Crawling: Smartsheet supports both local and federated users/groups, but the connector does not support federated. Usernames in Smartsheet are case-insensitive and allow special characters. This system ensures that two users can have the same name but must have unique email addresses. In addition, group names must be unique, because Smartsheet does not allow duplicate group names with mixed case. This prevents identity collisions, ensuring that permissions and access remain properly assigned. If an identity is deleted and later recreated, it does not automatically inherit previous permissions. Smartsheet does not have a suspended user concept, if a user is removed from the user library, they still appear in shared lists for sheets where they previously had access.

Permission Inheritance: Permissions in Smartsheet follow an inheritance model, where Workspaces act as the top-most entity. If no explicit ACL is set at the sheet or folder level, permissions are inherited from the parent Workspace. Inherited permissions typically operate as an intersection of parent permissions, unless explicitly modified. However, sheets can have their own ACLs that override inherited permissions. Document-level permissions can include options such as "View Sheet" or "Edit Sheet".

Change Management: Change Log Mode in Amazon Q Business enables incremental updates by capturing modifications made to content in Smartsheet. It indexes only newly added, updated, or deleted items since the last crawl, onstead of re-indexing all documents. Any changes to user or group access permissions are also recorded, ensuring accurate and up-to-date indexing.

Failure handling: The connector follows a fail-close approach, meaning if there are permission-related issues or API failures, affected documents are skipped from ingestion rather than being made publicly accessible. This prevents unauthorized access while maintaining data integrity.

For more information, see:

- Authorization

- Identity crawler
- Understanding User Store

IAM role for Smartsheet connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetS3Objects",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket/*"
      ],
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
```

```
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:us-west-2:111122223333:secret:QBusiness-
Smartsheet-Example-Secret"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-west-2:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:qbusiness:us-
west-2:111122223333:application/312ba974-4afc-8b7a-3180-6aec1db0d57c/
index/e2a71750-c4fd0-b34a-bf23-ddcce192d11d"
    },
    {
```

```
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:us-
west-2:111122223333:application/312ba974-4afc-8b7a-3180-6aec1db0d57c",
        "arn:aws:qbusiness:us-
west-2:111122223333:application/312ba974-4afc-8b7a-3180-6aec1db0d57c/
index/e2a71750-c4fd0-b34a-bf23-ddcce192d11d",
        "arn:aws:qbusiness:us-
west-2:111122223333:application/312ba974-4afc-8b7a-3180-6aec1db0d57c/
index/e2a71750-bf23-4fd0-b34a-192d11dddcce/data-source/*"
      ]
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAmazonQServicePrincipal",
            "Effect": "Allow",
            "Principal": {
                "Service": "qbusiness.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnEquals": {
```

```
                    "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
                }
            }
        }
    ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Connecting Zendesk to Amazon Q Business

Zendesk is a customer relationship management system that helps businesses automate and enhance customer support interactions. You can connect a Zendesk instance to Amazon Q Business—using either the AWS Management Console or the CreateDataSource API—and create an Amazon Q web experience.

Topics

- Known limitations for the Zendesk connector
- Zendesk connector overview
- Prerequisites for connecting Amazon Q Business to Zendesk
- Setting up Zendesk for connecting to Amazon Q Business
- Connecting Amazon Q Business to Zendesk using the console
- Connecting Amazon Q Business to Zendesk using APIs
- How Amazon Q Business connector crawls Zendesk ACLs
- Zendesk data source connector field mappings
- IAM role for the Zendesk connector
- Understand error codes in the Zendesk connector

Learn more

- For an overview of the Amazon Q web experience creation process using IAM Identity Center, see Configuring an application using IAM Identity Center.
- For an overview of the Amazon Q web experience creation process using AWS Identity and Access Management, see Configuring an application using IAM.
- For an overview of connector features, see Data source connector concepts.
- For information about connector configuration best practices, see Connector configuration best practices.

Known limitations for the Zendesk connector

The Zendesk connector has the following known limitations:

- Deleted and archived articles and their comments and attachments aren't supported in **Change log** mode since there are no SDK methods/REST API available for fetching deleted or archived articles.
- Archived articles aren't supported in **Full Crawl** mode since there are no SDK methods/REST API available for fetching archived articles.
- Deleted community topics, community posts, and their comments are not supported in **Change Log** mode since there are no SDK methods/REST API available for fetching deleted topics, deleted posts, and their comments.
- The Zendesk connector can't fetch community topics (added, edited, or deleted), and community posts and their comments (added, edited, or deleted) based on timestamps in **Change log** mode.
- When Access Control Lists (ACLs) are enabled, the "Sync only new or modified content" option is not available due to Zendesk API limitations. We recommend using "Full sync" or "New, modified, or deleted content sync" modes instead, or disable ACLs if you need to use this sync mode.

Zendesk connector overview

The following table gives an overview of the Zendesk connector and its supported features.

Category	Feature	Support
Security	**Authentication type**	OAuth 2.0 with implicit grant authentication, OAuth 2.0 authentication
	Authentication credentials	• OAuth 2.0 with Resource Owner Password Flow - Implicit grant token • OAuth 2.0 authentication - Zendesk Client ID • OAuth 2.0 authentication - Zendesk Client secret • OAuth 2.0 authentication - Zendesk Username • OAuth 2.0 authentication - Zendesk Password

Category	Feature	Support
	Access Control List (ACL) crawling	Yes. For more information, see ACL crawling.
	Identity crawling	Yes
	VPC	Yes
Crawl features	**Custom metadata**	Yes
	Entities	Yes. The following entities are supported: • Ticket • Ticket comment • Ticket comment attachment • Community topic • Community post • Community post comment • Article • Article attachment • Article comment **Note** Each instance of an entity is crawled as a single document. See What is a document? for more details on what each connector crawls as a document.
	Field mappings	Yes. Supports both default and custom field mappings. For more information, see Field mappings.

Category	Feature	Support
	Filters	Yes. The following filters are supported: • Organization name filter • Crawl tickets • Crawl ticket comments • Crawl ticket comment attachments • Crawl articles • Crawl article attachments • Crawl article comments • Crawl community topics • Crawl community posts • Crawl community post comments • Including and excluding content by file type • Including content based on a specific date
	Sync mode	Supports full and incremental sync.
	File types	Supports all files supported by Amazon Q.
	Crawled as a document	• Each ticket • Each ticket comment • Each ticket comment attachment • Each article • Each article attachment • Each article comment • Each community topic • Each community post • Each community post comment

Prerequisites for connecting Amazon Q Business to Zendesk

Before you begin, make sure that you have completed the following prerequisites.

In Zendesk, make sure you have:

- Created a Zendesk Suite (Professional/Enterprise) administrative account.
- Copied your Zendesk host URL. For example, *https://{sub-domain}.zendesk.com/*. You need this URL to allow Amazon Q to connect with your Zendesk data source.
- Generated Zendesk OAuth 2.0 with implicit grant credentials containing an implicit grant token.
- Generated Zendesk OAuth 2.0 credentials containing a client ID, client secret, username, and password. You need these credentials to authenticate Amazon Q to access Zendesk.

In your AWS account, make sure you have:

- Created a Amazon Q Business application.
- Created a Amazon Q Business retriever and added an index.
- Created an IAM role for your data source and, if using the Amazon Q API, noted the ARN of the IAM role.
- Stored your Zendesk authentication credentials in an AWS Secrets Manager secret and, if using the Amazon Q API, noted the ARN of the secret.

> **Note**
>
> If you're a console user, you can create the IAM role and Secrets Manager secret as part of configuring your Amazon Q application on the console.

For a list of things to consider while configuring your data source, see Data source connector configuration best practices.

Setting up Zendesk for connecting to Amazon Q Business

Before you connect Zendesk to Amazon Q Business, you need to create and retrieve the Zendesk credentials you will use to connect Zendesk to Amazon Q. You will also need to add any authorization permissions needed by Zendesk to connect to Amazon Q.

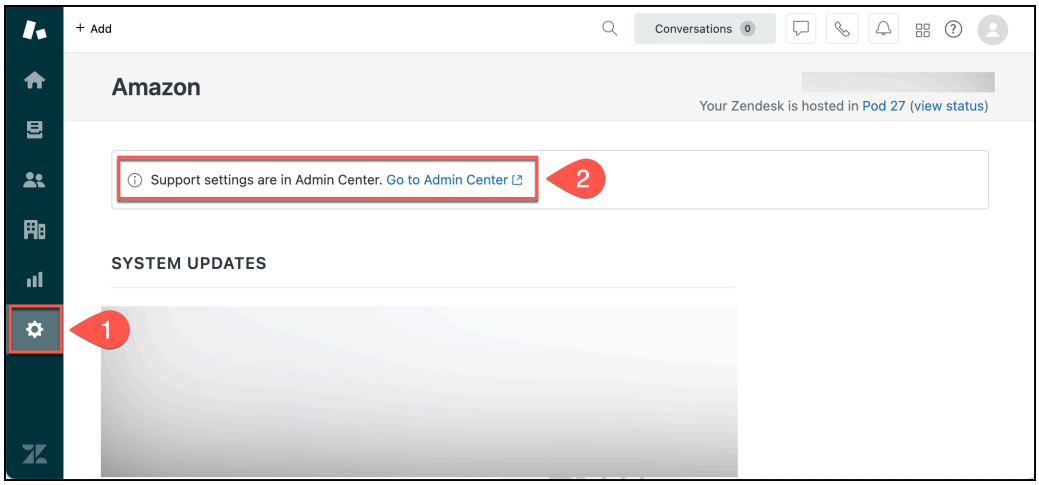
The following procedure gives you an overview of how to configure Zendesk for Amazon Q.

Configuring Zendesk for OAuth 2.0 authentication

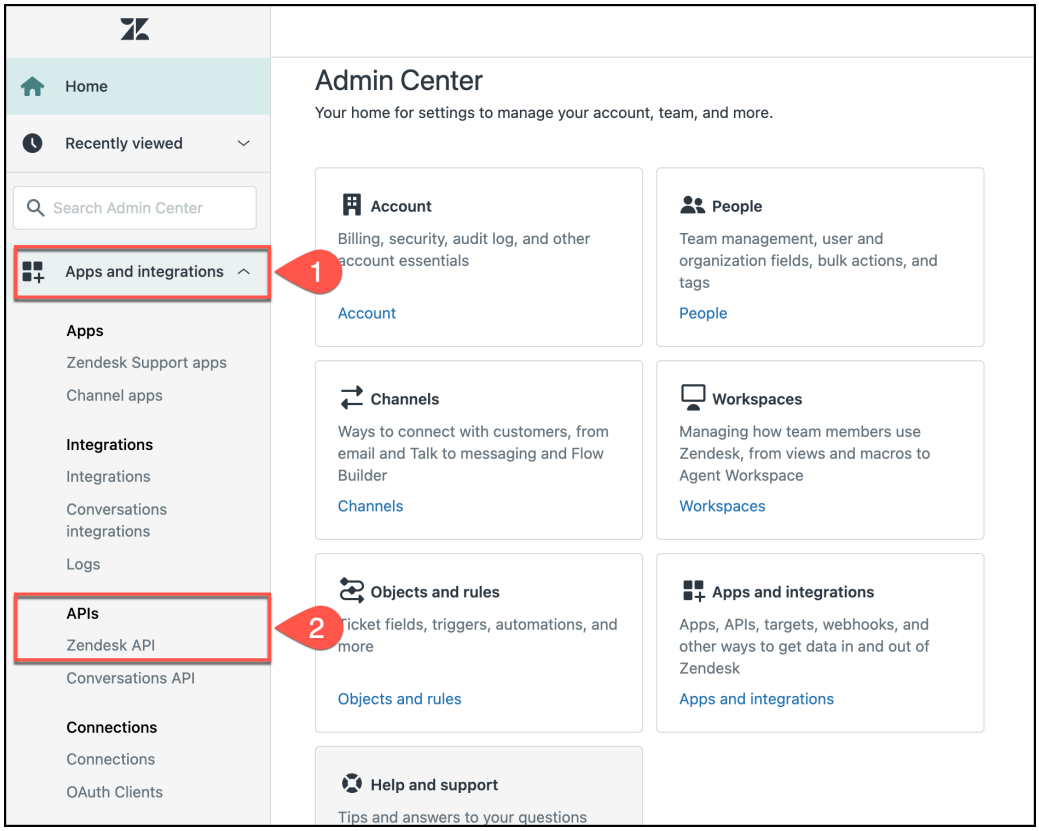
1. Log in to your Zendesk account. Note the username and password you logged in with. You will need them later to connect to Amazon Q.
2. Copy your Zendesk URL, if you haven't already, from the Zendesk webpage URL. This will be the URL you will input as host URL in Amazon Q.

> **Note**
>
> You can also copy your Zendesk host URL from the top menu in the **Admin Center**.

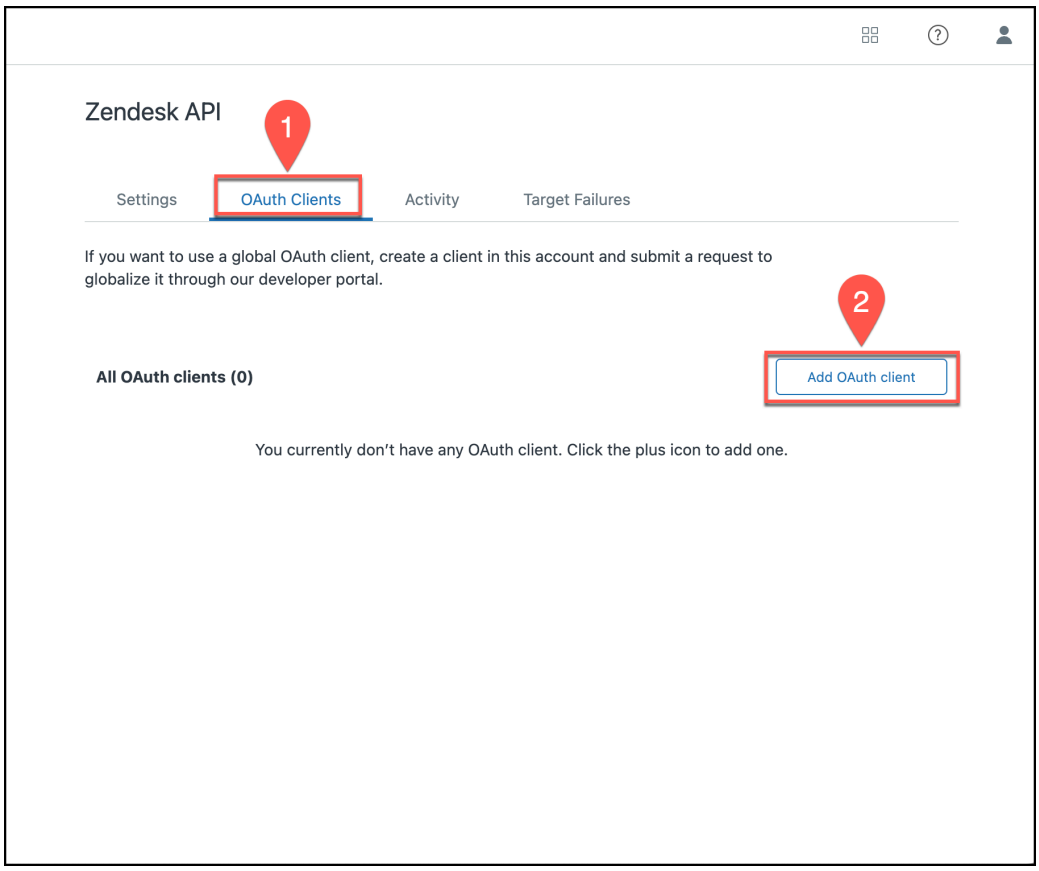
3. From the left navigation menu, choose the settings icon. Then, choose **Go to Admin Center**.



4. In **Admin Center**, from the left navigation menu, under **Apps and integrations**, choose **Zendesk API**.



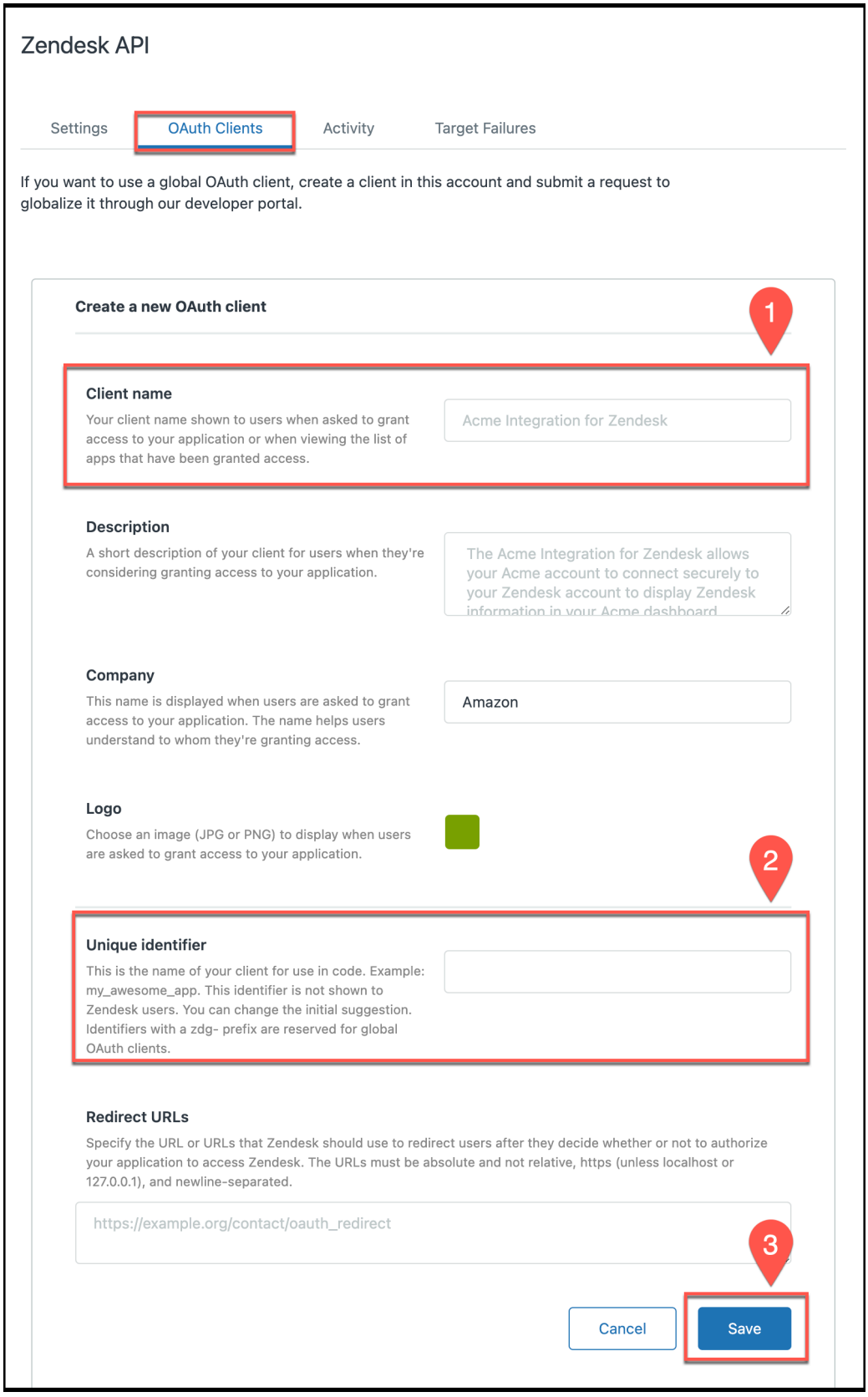
5. From the **Zendesk API** menu, choose **OAuth Clients** and then choose **Add OAuth client**.



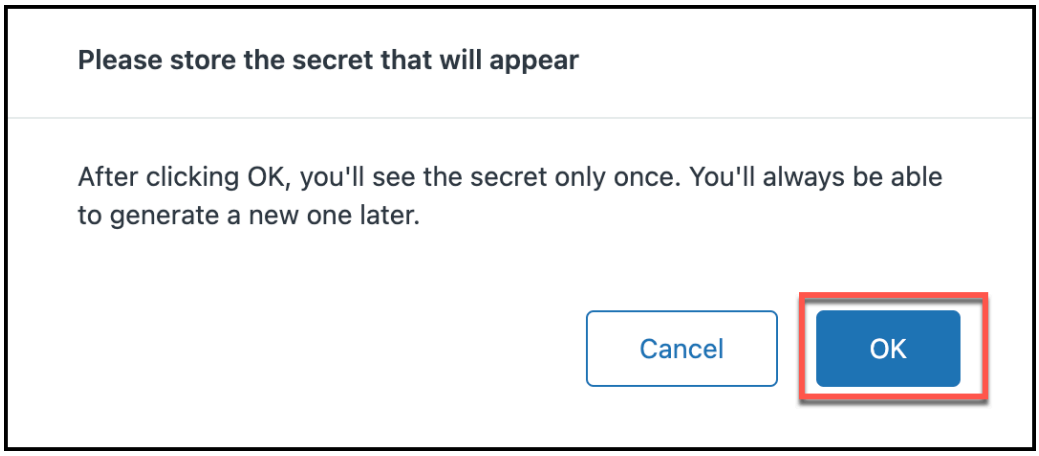
6. On the **OAuth Clients** page, under **Create a new OAuth client** enter the following information:

   - **Client name** – A human-readable name for your client. This will be visible to users.
   - **Unique identifier** – An internal code-level identifier for your client. This will be the Client ID you input in Amazon Q.

   Optionally, choose to fill in other information based on your use case. Then, choose **Save**.


Zendesk API
Settings
OAuth Clients
Activity
Target Failures
If you want to use a global OAuth client, create a client in this account and submit a request to globalize it through our developer portal.
Create a new OAuth client
1
Client name
Your client name shown to users when asked to grant access to your application or when viewing the list of apps that have been granted access.
Acme Integration for Zendesk
Description
A short description of your client for users when they're considering granting access to your application.
The Acme Integration for Zendesk allows your Acme account to connect securely to your Zendesk account to display Zendesk information in your Acme dashboard
Company
This name is displayed when users are asked to grant access to your application. The name helps users understand to whom they're granting access.
Amazon
Logo
Choose an image (JPG or PNG) to display when users are asked to grant access to your application.
2
Unique identifier
This is the name of your client for use in code. Example: my_awesome_app. This identifier is not shown to Zendesk users. You can change the initial suggestion. Identifiers with a zdg- prefix are reserved for global OAuth clients.
Redirect URLs
Specify the URL or URLs that Zendesk should use to redirect users after they decide whether or not to authorize your application to access Zendesk. The URLs must be absolute and not relative, https (unless localhost or 127.0.0.1), and newline-separated.
https://example.org/contact/oauth_redirect
3
Cancel
Save

7. On the **Please store the secret that will appear** dialog box that appears, select **OK**. Then, copy the secret you see into a text editor of your choice and save it. You won't be able to re-generate this secret so it's important that you store it securely. You will input this as the client secret during the connection configuration process in Amazon Q.



   You now have the username, password, host URL, client ID, and client secret you need to connect Zendesk to Amazon Q.

Connecting Amazon Q Business to Zendesk using the console

The following procedure outlines how to connect Amazon Q Business to Zendesk using the AWS Management Console.

Connecting Amazon Q to Zendesk

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Data sources**.
3. From the **Data sources** page, choose **Add data source**.
4. Then, on the **Add data sources** page, from **Data sources**, add the **Zendesk** data source to your Amazon Q application.
5. Then, on the **Zendesk** data source page, enter the following information:
6. **Name and description**, do the following:

   - For **Data source name** – Name your data source for easy tracking.

> **Note**
>
> You can include hyphens (-) but not spaces. Maximum of 1,000 alphanumeric characters.

- **Description – *optional*** – Add an optional description for your data source. This text is viewed only by Amazon Q Business administrators and can be edited later.

7. **Source** – Enter your **Zendesk URL**. For example, *https://{sub-domain}.zendesk.com/*.
8. **Authorization** – Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. If supported for your connector, you can manage ACLs by selecting **Enable ACLs** to enable ACLs or **Disable ACLs** to disable them. To manage ACLs, you need specific IAM permissions. See Grant permission to create data sources with ACLs disabled for more details. See Authorization for more details.
9. Authentication for existing Zendesk customers: Enter a name for your secret, a client ID, client secret, username, and password.
10. Authentication for new customers since 30 July 2024:

    a. Register the application with Zendesk and follow their procedure: Using OAuth authentication with your application

    b. Set Client kind to Confidential.

    c. For Redirect URL Enter the URL that Zendesk should use to grant access to the application. The URLs must be absolute and not relative. You can use localhost: `http://localhost` or `http://127.0.0.1`.

    d. Implement an OAuth authorization flow:

        1. Zendesk supports the authorization code grant flow to get access tokens. (Other grant flows have been deprecated.)
        2. The flow doesn't use refresh tokens. The access token doesn't expire.

    e. To get an authorization code, register users on the Zendesk authorization page: `https://{subdomain}.zendesk.com/oauth/authorizations/new`. Use the following parameters:

        1. `response_type` - Zendesk returns an authorization code in the response, so specify code as the response type. For example: response_type=code.

2. `redirect_url` - The URL, which can be local, that Zendesk should use to send the user's decision to grant access to your application. For example: `http://localhost` or `http://127.0.0.1`.
3. `client_id` - The unique identifier obtained after registering the application with Zendesk.
4. `scope` - A space-separated list of scopes that control access to the Zendesk resources.

f. After this, Zendesk will ask for user approval. Once approved it will respond with an authorization code.

g. Obtain an access token from Zendesk. Include the following parameters in the request:

1. `grant_type` - Specify `authorization_code` as the value.
2. `code` - Use the authorization code received from Zendesk after the user has been granted access.
3. `client_id` - Use the unique identifier specified in an OAuth client in the Support admin interface Admin > Channels > API > OAuth Clients.
4. `client_secret` - Use the secret specified in an OAuth client in the Support admin interface Admin > Channels > API > OAuth Clients).
5. `redirect_uri` - The URL, which can be local, that Zendesk should use to send the user's decision to grant access to your application. For example: `http://localhost` or `http://127.0.0.1`.
6. `scope` – A space-separated list of scopes that control access to the Zendesk resources.

For example:

```
curl https://{subdomain}.zendesk.com/oauth/tokens \
  -H "Content-Type: application/json" \
  -d '{"grant_type": "authorization_code", "code": "{your_code}",
    "client_id": "{your_client_id}", "client_secret": "{your_client_secret}",
    "redirect_uri": "{your_redirect_url}", "scope": "read" }' \
  -X POST
```

h. Use the access token in API calls.

11. **Configure VPC and security group – *optional*** – Choose whether you want to use a VPC. If you do, enter the following information:

a. **Subnets** – Select up to 6 repository subnets that define the subnets and IP ranges the repository instance uses in the selected VPC.

b. **VPC security groups** – Choose up to 10 security groups that allow access to your data source. Ensure that the security group allows incoming traffic from Amazon EC2 instances and devices outside your VPC. For databases, security group instances are required.

For more information, see VPC.

12. **IAM role** – Choose an existing IAM role or create an IAM role to access your repository credentials and index content.

> **Note**
>
> Creating a new service IAM role is recommended.

For more information, see IAM role.

13. **Sync scope** – Set the content that you want to sync.
14. For **Maximum file size** – Specify the file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
15. **Additional configuration – optional** – Configure the following settings:

- **Change log** – Select to update your index instead of syncing all your files.
- **Organization name** – Enter the Zendesk organization names to filter your sync.
- **Sync start date** – The date from which you want to index your content.
- **Regex patterns** – Regular expression patterns to include or exclude certain files. You can add up to 100 patterns.

16. **Advanced settings**

Document deletion safeguard - *optional*–To safeguard your documents from deletion during a sync job, select **On** and enter an integer between 0 - 100. If the percentage of documents to be deleted in your sync job exceeds the percentage you selected, the delete phase will be skipped and no documents from this data source will be deleted from your index. For more information, see Document deletion safeguard.

17. In **Sync run schedule**, for **Frequency** – Choose how often Amazon Q will sync with your data source. For more details, see Sync run schedule. To learn how to start a data sync job, see Starting data source connector sync jobs.
18. **Tags - *optional*** – Add tags to search and filter your resources or track your AWS costs. See Tags for more details.
19. **Field mappings** – A list of data source document attributes to map to your index fields.

> **Note**
>
> Add or update the fields from the **Data source details** page after you finish adding your data source. You can choose from two types of fields:

a. **Default** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can't edit these.

b. **Custom** – Automatically created by Amazon Q on your behalf based on common fields in your data source. You can edit these. You can also create and add new custom fields.

> **Note**
>
> Support for adding custom fields varies by connector. You won't see the **Add field** option if your connector doesn't support adding custom fields.

For more information, see Field mappings.

20. In **Data source details**, choose **Sync now** to allow Amazon Q to begin syncing (crawling and ingesting) data from your data source. When the sync job finishes, your data source is ready to use.

> **Note**
>
> View CloudWatch logs for your data source sync job by selecting **View CloudWatch logs**. If you encounter a `Resource not found exception` error, wait and try again as logs may not be available immediately.
> You can also view a detailed document-level report by selecting **View Report**. This report shows the status of each document during the crawl, sync, and index stages,

including any errors. If the report is empty for an in-progress job, check back later as data is emitted to the report as events occur during the sync process.
For more information, see Troubleshooting data source connectors.

Connecting Amazon Q Business to Zendesk using APIs

You use the CreateDataSource action to connect a data source to your Amazon Q application. You can also use the UpdateDataSource action to modify an existing data source configuration.

Then, you use the `configuration` parameter to provide a JSON blob that conforms the AWS-defined JSON schema.

For an example of the API request, see CreateDataSource and UpdateDataSource in the Amazon Q API Reference.

JSON schema

The following is the Zendesk JSON schema:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "hostUrl": {
              "type": "string",
              "pattern": "https:.*"
            }
          },
          "required": [
            "hostUrl"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
```

```
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "ticket": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": {
                "anyOf": [
                  {
                    "type": "object",
                    "properties": {
                      "indexFieldName": {
                        "type": "string"
                      },
                      "indexFieldType": {
                        "type": "string",
                        "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
                      },
                      "dataSourceFieldName": {
                        "type": "string"
                      },
                      "dateFieldFormat": {
                        "type": "string",
                        "pattern": "dd-MM-yyyy HH:mm:ss"
                      }
                    },
                    "required": [
                      "indexFieldName",
                      "indexFieldType",
                      "dataSourceFieldName"

                    ]
                  }
                ]
              }
            }
          },
          "required": [
            "fieldMappings"
          ]
        },
```

```
        "ticketComment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": {
                "anyOf": [
                  {
                    "type": "object",
                    "properties": {
                      "indexFieldName": {
                        "type": "string"
                      },
                      "indexFieldType": {
                        "type": "string",
                        "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
                      },
                      "dataSourceFieldName": {
                        "type": "string"
                      },
                      "dateFieldFormat": {
                        "type": "string",
                        "pattern": "dd-MM-yyyy HH:mm:ss"
                      }
                    },
                    "required": [
                      "indexFieldName",
                      "indexFieldType",
                      "dataSourceFieldName"

                    ]
                  }
                ]
              }
            }
          },
          "required": [
            "fieldMappings"
          ]
        },
        "ticketCommentAttachment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
```

```
            "type": "array",
            "items": {
              "anyOf": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "dd-MM-yyyy HH:mm:ss"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          }
        },
        "required": [
          "fieldMappings"
        ]
      },
      "article": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": {
              "anyOf": [
                {
                  "type": "object",
```

```
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "dd-MM-yyyy HH:mm:ss"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "communityPostComment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": {
            "anyOf": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
```

```
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "dd-MM-yyyy HH:mm:ss"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "articleComment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": {
            "anyOf": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
```

```
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "dd-MM-yyyy HH:mm:ss"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          }
        },
        "required": [
          "fieldMappings"
        ]
      },
      "articleAttachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": {
              "anyOf": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "dd-MM-yyyy HH:mm:ss"
                    }
```

```
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "communityTopic": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": {
            "anyOf": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "dd-MM-yyyy HH:mm:ss"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
```

```
                ]
              }
            ]
          }
        }
      },
      "required": [
        "fieldMappings"
      ]
    }
  }
},
"secretArn": {
  "type": "string",
  "minLength": 20,
  "maxLength": 2048
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "isCrawlAcl": {
      "type": "boolean"
    },
    "maxFileSizeInMegaBytes": {
      "type": "string"
    },
    "fieldForUserId": {
      "type": "string"
    },
    "organizationNameFilter": {
      "type": "array"
    },
    "sinceDate": {
      "type": "string",
      "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2} [0-9]{2}:[0-9]{2}:[0-9]{2}$"
    },
    "inclusionPatterns": {
      "type": "array"
    },
    "exclusionPatterns": {
      "type": "array"
    },
    "isCrawTicket": {
      "type": "string"
```

```
        },
        "isCrawTicketComment": {
          "type": "string"
        },
        "isCrawTicketCommentAttachment": {
          "type": "string"
        },
        "isCrawlArticle": {
          "type": "string"
        },
        "isCrawlArticleAttachment": {
          "type": "string"
        },
        "isCrawlArticleComment": {
          "type": "string"
        },
        "isCrawlCommunityTopic": {
          "type": "string"
        },
        "isCrawlCommunityPost": {
          "type": "string"
        },
        "isCrawlCommunityPostComment": {
          "type": "string"
        }
      }
    },
    "type": {
      "type": "string",
      "pattern": "ZENDESK"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FULL_CRAWL",
        "FORCED_FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "enableIdentityCrawler": {
      "type": "boolean"
    }
  },
  "version": {
```

```
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "additionalProperties": false,
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties",
    "syncMode",
    "secretArn",
    "type"
  ]
}
```

The following table provides information about important JSON keys to configure.

Configuration	Description
`connectionConfiguration`	Configuration information for the endpoint of the data source.
`repositoryEndpointMetadata`	The endpoint information for the data source.
`hostURL`	The Zendesk host URL. For example, *https://yoursubdomain.zendesk.com*.
`repositoryConfigurations`	Configuration information for the content of the data source. For example, configuring specific types of content and field mappings.
• `ticket` • `ticketComment` • `ticketCommentAttachment` • `article` • `articleComment` • `articleAttachment`	A list of Zendesk objects and their metadata attributes that Amazon Q crawls and maps to Amazon Q index field names. The Zendesk data source field names must exist in your Zendesk custom metadata.

Configuration	Description
• `communityTopic` • `communityPost` • `communityPostComment`	
`secretARN`	The Amazon Resource Name (ARN) of an AWS Secrets Manager secret that contains the key-value pairs required to connect to your Zendesk. The secret must contain a JSON structure with the following keys: host URL, client ID, client secret, username, and password.
`additionalProperties`	Additional configuration options for your content in your data source.
`isCrawlAcl`	`true` to crawl Access Control Lists. **Note** Amazon Q Business crawls ACL information by default to ensure responses are generated only from documents your end users have access to. See Authorization for more details.
`maxFileSizeInMegaBytes`	Specify the maximum single file size limit in MBs that Amazon Q will crawl. Amazon Q will crawl only the files within the size limit you define. The default file size is 50MB. The maximum file size should be greater than 0MB and less than or equal to 50MB.
`fieldForUserId`	Specify field to use for `UserId` for ACL crawling.

Configuration	Description
`organizationFilter`	If you want, you can choose to index tickets that exist within a specific **Organization**
`sinceDate`	If you want, you can configure a `sinceDate` parameter so that the Zendesk connector will crawl based on the `sinceDate` .
`inclusionPatterns`	A list of regular expression patterns to *include* specific files in your Zendesk data source. Files that match the patterns are included in the index. Files that don't match the patterns are excluded from the index. If a file matches both an inclusion and exclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.
`exclusionPatterns`	A list of regular expression patterns to *exclude* specific files in your Zendesk data source. Files that match the patterns are excluded from the index. Files that don't match the patterns are included in the index. If a file matches both an exclusion and inclusion pattern, the exclusion pattern takes precedence, and the file isn't included in the index.
• `isCrawlTicket` • `isCrawlTicketComment` • `isCrawlTicketCommentAttachment` • `isCrawlArticle` • `isCrawlArticleComment` • `isCrawlArticleAttachment` • `isCrawlCommunityTopic` • `isCrawlCommunityPost` • `isCrawlCommunityPostComment`	Input `true` to index these types of content.

Configuration	Description
type	Specify ZENDESK as your data source type.
syncMode	Specify whether Amazon Q should update your index by syncing all documents or only new, modified, and deleted documents. You can choose between the following options: • Use FORCED_FULL_CRAWL to freshly re-crawl all content and replace existing content each time your data source syncs with your index. • Use FULL_CRAWL to incrementally crawl only new, modified, and deleted content each time your data source syncs with your index. • Use CHANGE_LOG to incrementally crawl only new and modified content each time your data source syncs with your index.

Configuration	Description
`enableIdentityCrawler`	Specify `true` to activate identity crawler. Identity crawler is activated by default. Crawling identity information on users and groups with access to certain documents is useful for user context filtering. Search results are filtered based on the user or their group access to documents. **Note** Amazon Q Business crawls identity information from your data source by default to ensure responses are generated only from documents end users have access to. For more information, see Identity crawler.
`version`	The version of the template that's currently supported.

How Amazon Q Business connector crawls Zendesk ACLs

Connectors support crawling ACL and identity information where applicable based on the data source. If you index documents without ACLs, all documents are considered public. Indexing documents with ACLs ensures data security.

Amazon Q Business supports crawling ACLs for document security by default.

When you connect an Zendesk data source to Amazon Q Business, Amazon Q Business crawls ACL information attached to a document (user and group information) from your Zendesk instance. If you choose to activate ACL crawling, the information can be used to filter chat responses to your end users' document access level.

The Zendesk connector supports enabling or disabling data ingestion for various entities including Tickets, Ticket Comments, Ticket Comment Attachments, Articles, Article Attachments, Article Comments, Community Topics, Community Posts, and Community Post Comments. For Ticket

Comment Attachments and Article Attachments, the Zendesk connector allows applying include/exclude patterns based on file types, enabling more granular control over which attachments are ingested into Amazon Q Business.

Roles/Permissions: Zendesk roles define user permissions within the platform, including Admins, Agents, Light Agents, End Users, and Guide Admins. Admins have full control over settings, user management, and content access. Agents handle tickets, respond to customer queries, and may have restricted access based on group assignments. Light Agents can view and comment on tickets internally but cannot interact with customers. End Users are customers who can submit and track tickets. Guide Admins manage knowledge base content, including articles and community posts. Access control is determined by roles, groups, organizations, and user segments, ensuring the right level of visibility and permissions across the system. The Zendesk connector translates these roles into Amazon Q Business compatible ACLs, supporting View (Read), Edit, and Delete permissions.

Identity Crawling: The connector ensures accurate synchronization of user access control by retrieving and updating user identities, groups, and permissions. During this process, it fetches users from Zendesk Organizations, Groups, and User Segments, aligning them with the correct Access Control Lists (ACLs) in Amazon Q Business. This allows for consistent enforcement of role-based access, ensuring that users can only view content they are permitted to access. Additionally, identity crawling updates group memberships dynamically, reflecting changes in user roles, suspended accounts, and newly assigned permissions during scheduled syncs.

Permissions Inheritance: In Zendesk, permission inheritance varies across data source entities such as tickets, articles, and community content. For tickets, permissions are inherited based on roles (Requester, Assignee, Follower) and group or organization membership. Permissions for comments, notes and attachments of tickets are inherited from parent. Community topics and posts inherit permissions from assigned user segments, but Admins and Guide Admins have universal access.

Change Management: Change Log Mode in Amazon Q Business enables incremental updates by capturing modifications made to content in Zendesk. Instead of re-indexing all documents, it indexes only newly added, updated, or deleted items since the last crawl. Any changes to user or group access permissions are also recorded, ensuring accurate and up-to-date indexing. However, change log sync does not update ACLs for suspended or reactivated users.

Failure Handling: The connector follows a fail-close approach, meaning if there are permission-related issues or API failures, affected documents are skipped from ingestion rather than being made publicly accessible. This prevents unauthorized access while maintaining data integrity.

For more information, see:

- Authorization
- Identity crawler
- Understanding User Store

Zendesk data source connector field mappings

To improve retrieved results and customize the end user chat experience, Amazon Q Business enables you to map document attributes from your data sources to fields in your Amazon Q index.

Amazon Q offers two kinds of attributes to map to index fields:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data source to Amazon Q index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q index fields.

When you connect Amazon Q to a data source, Amazon Q automatically maps specific data source document attributes to fields within an Amazon Q index. If a document attribute in your data source doesn't have a attribute mapping already available, or if you want to map additional document attributes to index fields, use the custom field mappings to specify how a data source attribute maps to an Amazon Q index field. You create field mappings by editing your data source after your application and retriever are created.

To learn more about document attributes and how they work in Amazon Q, see Document attributes and types in Amazon Q.

> **Important**
>
> Filtering using document attributes in chat is only supported through the API.

The Amazon Q Zendesk connector supports the following entities and the associated reserved and custom attributes.

Supported entities and field mappings

- Tickets

- Ticket comments
- Ticket comment attachment
- Article
- Article comment
- Article comment attachment
- Community topic
- Community post
- Community post comment

Tickets

Amazon Q supports crawling Zendesk Tickets and offers the following ticket field mappings.

Zendesk field name	Index field name	Description	Data type
ticketChannel	zd-channel	Custom	String
category	_category	Default	String
authors	_authors	Default	String list
assignee	zd_assignee	Custom	String
tags	zd_tags	Custom	String list
status	zd_status	Custom	String
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
organizationName	zd_organization_name	Custom	String

Ticket comments

Amazon Q supports crawling Zendesk Ticket Comments and offers the following ticket comment field mappings.

Zendesk field name	Index field name	Description	Data type
category	_category	Default	String
authors	_authors	Default	String list
status	zd_status	Custom	String
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
organizationName	zd_organization_name	Custom	String

Ticket comment attachment

Amazon Q supports crawling Zendesk Ticket Comment Attachments and offers the following ticket comment attachment field mappings.

Zendesk field name	Index field name	Description	Data type
category	_category	Default	String
authors	_authors	Default	String list
status	zd_status	Custom	String
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date

Zendesk field name	Index field name	Description	Data type
organizationName	zd_organization_name	Custom	String

Article

Amazon Q supports crawling Zendesk Articles and offers the following article field mappings.

Zendesk field name	Index field name	Description	Data type
authors	_authors	Default	String list
labels	zd_article_labels	Custom	String list
section	zd_article_section	Custom	String list
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date

Article comment

Amazon Q supports crawling Zendesk Article Comments and offers the following article comment field mappings.

Zendesk field name	Index field name	Description	Data type
authors	_authors	Default	String list
labels	zd_article_labels	Custom	String list
section	zd_article_section	Custom	String list
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date

Zendesk field name	Index field name	Description	Data type
updatedAt	_last_updated_at	Default	Date

Article comment attachment

Amazon Q supports crawling Zendesk Article Comment Attachments and offers the following article comment attachment field mappings.

Zendesk field name	Index field name	Description	Data type
authors	_authors	Default	String list
labels	zd_article_labels	Custom	String list
fileName	zd_file_name	Custom	String
fileType	_file_type	Default	String
fileSize	zd_file_size	Custom	Long (numeric)
section	zd_article_section	Custom	String list
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date

Community topic

Amazon Q supports crawling Zendesk Community Topics and offers the following community topic field mappings.

Zendesk field name	Index field name	Description	Data type
topicName	zd_topic_name	Custom	String
sourceUrl	_source_uri	Default	String

Zendesk field name	Index field name	Description	Data type
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
category	_category	Default	String

Community post

Amazon Q supports crawling Zendesk Community Posts and offers the following community post field mappings.

Zendesk field name	Index field name	Description	Data type
postName	zd_post_name	Custom	String
topicName	zd_topic_name	Custom	String
sourceUrl	_source_uri	Default	String
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
category	_category	Default	String

Community post comment

Amazon Q supports crawling Zendesk Community Post Comments and offers the following community post comment field mappings.

Zendesk field name	Index field name	Description	Data type
postName	zd_post_name	Custom	String
topicName	zd_topic_name	Custom	String
sourceUrl	_source_uri	Default	String

Zendesk field name	Index field name	Description	Data type
createdAt	_created_at	Default	Date
updatedAt	_last_updated_at	Default	Date
category	_category	Default	String

IAM role for the Zendesk connector

If you use the AWS CLI or an AWS SDK, you must create an AWS Identity and Access Management (IAM) policy before you create an Amazon Q resource. When you call the CreateDataSource operation, you provide the Amazon Resource Name (ARN) role with the policy attached.

If you use the AWS Management Console, you can create a new IAM role in the Amazon Q console or use an existing IAM role.

To learn more about IAM roles, see IAM roles in the *AWS Identity and Access Management User Guide*.

To connect your data source connector to Amazon Q, you must give Amazon Q an IAM role that has the following permissions:

- Permission to access the `BatchPutDocument` and `BatchDeleteDocument` operations to ingest documents.
- Permission to access the User Store API operations to ingest user and group access control information from documents.
- Permission to access your AWS Secrets Manager secret to authenticate your data source connector instance.
- **(Optional)** If you're using Amazon VPC, permission to access your Amazon VPC.

```
{
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQToGetSecret",
      "Effect": "Allow",
      "Action": [
```

```
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToDecryptSecret",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToIngestDocuments",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument",
        "qbusiness:BatchDeleteDocument"
      ],
      "Resource": [
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}",
      "arn:aws:qbusiness:{{region}}:{{source_account}}:application/{{application_id}}/
index/{{index_id}}"
      ]
    },
    {
      "Sid": "AllowsAmazonQToIngestPrincipalMapping",
      "Effect": "Allow",
      "Action": [
        "qbusiness:PutGroup",
        "qbusiness:CreateUser",
        "qbusiness:DeleteGroup",
        "qbusiness:UpdateUser",
```

```
        "qbusiness:ListGroups"
      ],
      "Resource": [
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}",
        "arn:aws:qbusiness:{{region}}:{{account_id}}:application/{{application_id}}/
index/{{index_id}}/data-source/*"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNI",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[subnet_ids]]",
        "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[security_group]]"
      ]
    },
    {
      "Sid": "AllowsAmazonQToCreateAndDeleteNIForSpecificTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AMAZON_Q"
          ]
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateTags",
      "Effect": "Allow",
```

```
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid": "AllowsAmazonQToCreateNetworkInterfacePermission",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AMAZON_Q": "qbusiness_{{account_id}}_{{application_id}}_*"
        }
      }
    },
   {
      "Sid": "AllowsAmazonQToDescribeResourcesForVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    }
  ]
}
```

To allow Amazon Q to assume a role, you must also use the following trust policy:

```
{
```

```
  "Version": "2012-10-17",       ,
  "Statement": [
    {
      "Sid": "AllowsAmazonQServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:qbusiness:{{region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

For more information on Amazon Q data source connector IAM roles, see IAM roles for Amazon Q data source connectors.

Understand error codes in the Zendesk connector

The following table provides information about error codes you may see for the Zendesk connector and suggested resolutions.

Error code	Error message	Suggested resolution
ZND-5001	Error validating credentials due to invalid username or password.	Provide a valid username/password.
ZND-5002	Error validating credentials due to invalid client Id or client Secret.	Provide a valid Zendesk client Id or client Secret.

Error code	Error message	Suggested resolution
ZND-5100	The host URL is null or empty.	Provide a valid host Url.
ZND-5101	The username is null or empty.	Provide a valid username.
ZND-5102	The password is null or empty.	Provide a valid password.
ZND-5103	The Zendesk client Id is null or empty.	Provide a valid client Id.
ZND-5104	The Zendesk client Secret is null or empty.	Provide a valid client Secret.
ZND-5105	Invalid date format for field 'sinceDate'.	Date format should be yyyy-MM-dd HH:mm:ss.
ZND-5106	Invalid value for field 'sinceDate'.	Since date should not be greater than the current date.
ZND-5107	The datatype for the index field is invalid.	Only String, Date and Long formats are supported for field mappings.
ZND-5108	The isCrawTicket value is invalid.	isCrawTicket should be a boolean value true or false.
ZND-5109	The isCrawTic ketComment value is invalid.	isCrawTicketComment should be a boolean value true or false.
ZND-5110	The isCrawTic ketCommentAttachment value is invalid.	isCrawTicketCommentAttachment should be a boolean value true or false.
ZND-5111	The isCrawlArticle value is invalid.	isCrawlArticle should be a boolean value true or false.

Error code	Error message	Suggested resolution
ZND-5112	The isCrawlArticleComment value is invalid.	isCrawlArticleComment should be a boolean value true or false.
ZND-5113	The isCrawlArticleAttachment value is invalid.	isCrawlArticleAttachment should be a boolean value true or false.
ZND-5114	The isCrawlCommunityTopic value is invalid.	isCrawlCommunityTopic should be a boolean value true or false.
ZND-5115	The isCrawlCommunityPost value is invalid.	isCrawlCommunityPost should be a boolean value true or false.
ZND-5116	The isCrawlCommunityPostComment value is invalid.	isCrawlCommunityPostComment should be a boolean value true or false.
ZND-5117	Repository Configurations is null or empty.	Repository Configurations should not be null or empty value.
ZND-5118	The Host Url pattern is not valid.	Provide a valid host url. Ex: 'https://{sub-domain}.zendesk.com/' or 'https://{sub-domain}.zendesk.com'
ZND-5119	The URI is invalid.	Provide a valid URI.
ZND-5120	The personal access token is null or empty.	Provide a valid patToken.
ZND-5121	The auth type is incorrect.	The auth type should be OAuth2 or Oauth2-ImplicitGrantFlow.
ZND-5122	The accessToken provided is expired, revoked, malformed or invalid.	Provide valid accessToken.

Error code	Error message	Suggested resolution
ZND-5123	The access token doesn't have sufficient permissio n.	Check the user has sufficient permissio n to crawl.
ZND-5500	Unable to fetch data from Zendesk.	Check your Zendesk account plan/subs cription: it may have expired.
ZND-5501	Unable to generate access token.	Check your Zendesk configuration and try again.
ZND-5502	There was an error parsing the field value. The size has exceeded the maximum allowable limit.	The maximum size permitted is 1000 characters for the fields.
ZND-5503	The url is invalid.	Provide valid URL.

Understanding Amazon Q Business User Store

With the Amazon Q Business *User Store* feature, end users see Amazon Q Business chat responses generated *only* from the documents that they have access to within an Amazon Q Business application. To achieve this, Amazon Q creates a mapping within the data sources attached to that application. The mapping is between every unique user accessing the application environment and all the user IDs and user groups that they are associated with. Amazon Q Business stores this principal mapping information in its internal User Store. During chat, Amazon Q Business uses the mapping information to return answers that are scoped to a user's identity.

When you use the API, you use the User Store API actions to customize and configure your user management solution. For more details, see Using User Store APIs.

When you use the console, Amazon Q Business automatically crawls user and group information during the connector setup process. You can't create, add, or customize users and groups to the user store using the AWS Management Console.

Note

As of Dec 17, 2024, Amazon Q Business will recognize all email addresses as case-insensitive and recognize subaddresses as equivalent to the original email address. For example, JohnDoe@example.com, johndoe@example.com, and johndoe +work@example.com will be considered the same email address. For assistance with applications or to report a concern, contact Support sign into the AWS Support Center .

Note

The User Store feature is not available for the Amazon S3 and Amazon Q Web Crawler connectors that are used with Amazon Q Business. For more information about using access control information for user identity specific chat responses for these connectors, see Amazon S3 and Amazon Q Business Web Crawler.

Topics

- Principal mapping
- How the User Store works

Principal mapping

Amazon Q Business uses *principal mapping* to map users and groups with permissions to access an Amazon Q Business application environment to their user ids and group membership information within the data sources that are connected to the application.

Although user and group mapping is a synchronous, simultaneous process, the following sections explain them separately for conceptual clarity.

Topics

- User mapping
- Group mapping

User mapping

Each Amazon Q Business application environment can have multiple data sources connected to it. Each data source can have specific users and groups configured within it. Additionally, a user can be associated with multiple groups within a data source, or be attached to multiple groups across multiple data sources. A user attached to multiple data sources can also have different user IDs within these data sources.

A unique end user who signs in to an Amazon Q Business application environment must see only chat responses generated from documents that they have access to. To achieve that objective, Amazon Q Business maps their user IDs and group IDs within each data source to their identity provider (IdP) login credentials. Then, Amazon Q Business creates a universally unique identifier (UUID) to assign to each user. Using the UUID that it creates, Amazon Q Business stores a comprehensive mapping of the user's group membership in an application. During chat, Amazon Q Business checks this UUID that's stored in its user store and retrieves user access information to generate chat responses.

The User Store feature also supports the following user management scenarios:

- **An end user leaves your organization.**

  When an end user leaves your organization, you can choose to delete the user from your user store.
- **An end user leaves your organization, and their email gets reassigned.**

  Because the User Store assigns each user a UUID for secure and accurate chat responses, using an email reassigned from a previous UUID to a new one doesn't impact the content that a user sees. Any new user within your application environment that is using a reassigned email ID will be assigned a new UUID to be used for response generation.
- **An end user with multiple login IDs needs chat content generated from documents they access using both these login IDs.**

  With User Store, you can store user aliases attached to end user UUIDs. For example, a username Saanvi Sarkar uses two login IDs to sign in to Amazon Q Business—`saanvi_sarkar` and `saanvi_s`. You can store both IDs under the same UUID to ensure their chat responses are generated from content that they access using both login IDs.

Group mapping

Each Amazon Q Business application environment can have multiple data sources attached to it. Each data source in an Amazon Q Business application environment can have multiple groups attached to it. Multiple groups can repeat across multiple data sources. Additionally, each group across data sources can also contain multiple subgroups. Each Amazon Q Business application environment also has an associated identity provider (IdP) that can contain group information for the users accessing the application.

A unique end user signing in to an Amazon Q Business application environment must see only chat responses generated from documents within groups that they have access to. To achieve that objective, Amazon Q Business does the following:

- Automatically crawls local groups and their associated relationships from data sources during the connector configuration process.
- Provides you with API operations to map your end users group and subgroup membership details within each data source to their IdP group membership.

> **Note**
>
> As of Dec 17, 2024, Amazon Q Business will recognize all email addresses as case-insensitive and recognize subaddresses as equivalent to the original email address. For example, JohnDoe@example.com, johndoe@example.com, and johndoe+work@example.com will be considered the same email address. For assistance with applications or to report a concern, contact Support, sign into the AWS Support Center .

Then, Amazon Q Business creates a unique user identifier (UUID) to assign to each user. Under the UUID, Amazon Q Business stores a comprehensive mapping of the user's group membership in an application. During chat, Amazon Q Business checks this UUID that's stored in its user store and quickly retrieves group access information to generate chat responses.

The User Store feature supports the following group management scenarios:

- **Your users mapped to all groups that they have access to within an Amazon Q Business application.**

Amazon Q Business crawls all groups that a user has access to in a data source and stores this information under a user's UUID.

- **Create a subgroup of users within your application.**

  For example, for a group called `company_employees`, you might want to create a subgroup `summer_interns` and specify group level access for the subgroup. You might also want to group your interns into further subgroups like `product_interns` and `engineering_interns`.

- **Map your data source groups to your IdP groups.**

  A unique end user signing in to an Amazon Q Business application must see only chat responses generated from documents within groups they have access to. To support that objective, you can use Amazon Q to map your end users group membership details within each data source to their IdP group membership.

  > **Note**
  >
  > Amazon Q Business doesn't interact or crawl this information from your IdP automatically. To ingest the relationship between data source groups and IdP groups, use the Amazon Q Business API.

How the User Store works

Each document in any data source has access control list (ACL) information inherently attached to it as metadata. ACLs contain information about which users and groups have access to a document.

Connectors support crawl ACL and identity information where applicable based on the data source. To index documents without ACLs (as public documents) ensure the documents you want to index from your data source are public documents in the enterprise data source the connectors index the content from.

An Amazon Q Business connector updates any changes in ACLs each time that your data source content is crawled. To capture ACL changes to make sure that the right end users have access to the right content, re-sync your data source regularly.

Note

As of Dec 17, 2024, Amazon Q Business will recognize all email addresses as case-insensitive and recognize subaddresses as equivalent to the original email address. For example, JohnDoe@example.com, johndoe@example.com, and johndoe+work@example.com will be considered the same email address. For assistance with applications or to report a concern, contact Support, sign into the AWS Support Center .

Note

Amazon Q Business supports crawling ACLs for document security by default. As a general rule, turning off ACLs and identity crawling once they have been enabled are no longer supported. In preparation for connecting Amazon Q Business applications to IAM Identity Center, enable ACL indexing and identity crawling for secure querying and re-sync your connector. Once you turn ACL and identity crawling on you won't be able to turn them off. Certain connectors provide you with the ability to manage ACLs by enabling or disabling them during data source creation. To create a data source with ACLs disabled, you need specific IAM permissions. For more information, see Setting up.

Each data source also contains information about the users and groups which have access to it. Amazon Q Business crawls information about users and groups attached to each data source and automatically extracts and maps user and group information internally. Amazon Q Business then stores this crawled identity information in the user store and uses it to match and map user and group IDs with their document access details.

If you delete a group in the User Store and then re-create it later with the same name but with different group members, document ACLs which contain this group may be impacted. We recommend that this type of change (deleting or re-creating a group with the same name but with different group members) be done in the data source instead of the Amazon Q Business User Store.

Using a reassigned email address requires deleting the original user's UUID from the User Store. This is because Amazon Q Business verifies that the new user's IAM Identity Center attributes match those in the User Store. If the previous email address user UUID is not deleted, and the previous user's attributes are found, API calls will be denied.

Important

Inadvertent mistakes when you update the User Store's user, group, group membership, and mapping information can result in unintentional and unacceptable changes in the accessibility of documents to users.
Treat the ability to update the User Store to create users, update users, delete users, create groups, update groups, delete groups (i.e, create update delete operations), and update the mappings, as a privileged operation.
Ensure that access to the User Store APIs is provided only to admin who fully understand how to use these APIs and the implications of these changes on your document security.
We recommend establishing a documented approval process be followed for making such changes.

The following overview describes how principal mapping works by using either the console or the Amazon Q Business API.

Topics

- Using the console
- Using the API

Using the console

Each document in any data source has access control list (ACL) information inherently attached to it as metadata. ACLs contain information about which users and groups have access to a document. To ensure document security, Amazon Q Business crawls ACL information by default. Then, the connector automatically extracts and maps document access information internally.

When you crawl this ACL information, Amazon Q Business stores it in its internal user store to assess which user IDs have access to a document.

Each data source also contains information about the users and groups which have access to it. During data source connector configuration, Amazon Q Business crawls information about users and groups attached to each data source. Then, the connector automatically extracts and maps user and group information internally.

Amazon Q Business stores this crawled identity information in the user store and uses it to match and map user and group ids with their document access details. You can only use the **Identity crawler** feature if you also crawl ACLs using the **Authorization** feature.

If you use the console, you must re-sync your data to your index to capture any changes in the ACL and user and group membership within your data source.

For more information regarding setting up user mapping for specific connectors, consult the detailed ACL crawling documentation section for that connector. For example, if you need to set up user mapping for Salesforce Online, see the section called “ACL crawling”.

Using the API

When you configure your Amazon Q Business application, you use the following API operations to create your principal mapping solution:

User management

- CreateUser – Creates a universally unique identifier (UUID) that's mapped to a list of local user IDs within a data source.
- DeleteUser — Deletes a UUID that's mapped to a user.
- UpdateUser – Updates local user IDs within a data source that are mapped to a UUID.
- GetUser – Lists information associated with a user ID.

Group management

- PutGroup – Creates, or updates, a mapping of users to groups, or groups to subgroups. You can use this API operation to:
  - Map a group from groups in the data source to groups in your IdP.
  - Map a list of users and sub groups (for example, `Interns`) to a group (for example, `Interns 2023`).
- DeleteGroup – Deletes a group or a subgroup.
- GetGroup – Lists information about a group.

Using Amazon VPC with Amazon Q Business connectors

Amazon Q Business can connect to a virtual private cloud (VPC) that you created with Amazon Virtual Private Cloud to index content stored in data sources running in your private cloud. When

you create a data source connector, you can provide security group and subnet identifiers for the subnet that contains your data source. With this information, Amazon Q Business creates an elastic network interface that it uses to securely communicate with your data source within your VPC.

To set up an Amazon Q Business data source connector with Amazon VPC, you can use either the AWS Management Console or the CreateDataSource API operation. If you use the console, you connect a VPC during the connector configuration process.

> **Note**
>
> The Amazon VPC feature is optional when setting up an Amazon Q Business data source connector. If your data source is accessible from the public internet, you don't need to enable the Amazon VPC feature. Not all Amazon Q Business data source connectors support Amazon VPC.

If your data source isn't running on Amazon VPC and isn't accessible from the public internet, you first connect your data source to your VPC using a virtual private network (VPN). Then, you can connect your data source to Amazon Q Business by using a combination of Amazon VPC and AWS Virtual Private Network. For information about setting up a VPN, see the Site-to-Site VPN documentation.

Topics

- Configuring Amazon VPC support for Amazon Q Business connectors
- Set up an Amazon Q Business data source to connect to Amazon VPC
- Viewing Amazon VPC identifiers
- Checking your data source IAM role
- Using Amazon VPC with an Amazon S3 data source
- Step 3. Configure your external data source and Amazon VPC

Configuring Amazon VPC support for Amazon Q Business connectors

To configure Amazon VPC for use with your Amazon Q Business connectors, take the following steps.

Steps

- Step 1. Create Amazon VPC subnets for Amazon Q Business

- Step 2. Create Amazon VPC security groups for Amazon Q Business
- Step 3. Configure your external data source and Amazon VPC

Step 1. Create Amazon VPC subnets for Amazon Q Business

Create or choose an existing Amazon VPC subnet that Amazon Q Business can use to access your data source. The prepared subnets must be in one of the following AWS Regions and Availability Zones:

- US West (Oregon)/us-west-2—usw2-az1, usw2-az2, usw2-az3
- US East (N. Virginia)/us-east-1—use1-az1, use1-az2, use1-az4
- Europe (Ireland)/eu-west-1—euw1-az1, euw1-az2, euw1-az3
- Asia Pacific (Sydney)/ap-southeast-2—apse2-az1, apse2-az2, apse2-az3

Your data source must be accessible from the subnets that you provided to Amazon Q Business connector.

For more information about how to configure Amazon VPC subnets, see Subnets for your Amazon VPC in the *Amazon VPC User Guide*.

If Amazon Q Business must route the connection between two or more subnets, you can prepare multiple subnets. For example, the subnet that contains your data source is out of IP addresses. In that case, you can provide Amazon Q with an additional subnet that has sufficient IP addresses and connected to the first subnet. If you list multiple subnets, the subnets must be able to communicate with each other.

Step 2. Create Amazon VPC security groups for Amazon Q Business

To connect your Amazon Q Business data source connector to Amazon VPC, you must prepare one or more security groups from your VPC to assign to Amazon Q Business. The security groups will be associated to the elastic network interface created by Amazon Q Business. This network interface controls inbound and outbound traffic to and from Amazon Q Business when accessing the Amazon VPC subnets.

Make sure that your security group's outbound rules allow the traffic from Amazon Q Business data source connectors to access the subnets and the data source that you are going to sync with. For example, you might use an MySQL connector to sync from a MySQL database. If you're using the

default port, the security groups must allow Amazon Q to access port 3306 on the host that runs the database.

We recommend that you configure a default security group with the following values for Amazon Q Business to use:

- **Inbound rules** – If you choose to leave this empty, all inbound traffic will be blocked.
- **Outbound rules** – Add one rule to allow all outbound traffic so that Amazon Q Business can initiate the requests to sync from your data source.
  - **IP version** – IPv4
  - **Type** – All traffic
  - **Protocol** – All traffic
  - **Port range** – All
  - **Destination** – 0.0.0.0/0

For more information about how to configure Amazon VPC security groups, see Security group rules in the *Amazon VPC User Guide*.

Step 3. Configure your external data source and Amazon VPC

Make sure that your external data source has the correct permissions configuration and network settings for Amazon Q Business to access it. You can find detailed instructions on how to configure your data sources in the prerequisites section of each connector page.

Also, check your Amazon VPC settings and make sure that your external data source is reachable from the subnet you will assign to Amazon Q Business. To do this, we recommend that you create an Amazon EC2 instance in the same subnet with the same security groups and test access to your data source from this Amazon EC2 instance. For more information, see Troubleshooting Amazon VPC connection.

Set up an Amazon Q Business data source to connect to Amazon VPC

When you add a new data source in Amazon Q Business, you can use the Amazon VPC feature if the selected data source connector supports this feature.

You can set up a new Amazon Q Business data source with Amazon VPC enabled by using the AWS Management Console or the Amazon Q Business API. Specifically, use the CreateDataSource API operation, and then use the `VpcConfiguration` parameter to provide the following information:

- `SubnetIds` – A list of identifiers of Amazon VPC subnets
- `SecurityGroupIds` – A list of identifiers of Amazon VPC security groups

If you use the console, you provide the required Amazon VPC information during connector configuration. To use the console to enable the Amazon VPC feature for a connector, you first choose an Amazon VPC. Then, you provide identifiers of any Amazon VPC subnets and identifiers of any Amazon VPC security groups. You can choose the Amazon VPC subnets and Amazon VPC security groups that you created in Configuring Amazon VPC, or use any existing ones.

Topics

- Viewing Amazon VPC identifiers
- Checking your data source IAM role
- Using Amazon VPC with an Amazon S3 data source
- Step 3. Configure your external data source and Amazon VPC

Viewing Amazon VPC identifiers

The identifiers for subnets and security groups are configured in the Amazon VPC console. To view the identifiers, use the following procedures.

To view subnet identifiers

1. Sign in to the AWS Management Console and open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. From the navigation pane, choose **Subnets**.
3. From the **Subnets** list, choose the subnet that contains your database server.
4. From the **Details** tab, make a note of the identifier in the **Subnet ID** field.

To view security group identifiers

1. Sign in to the AWS Management Console and open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. From the navigation pane, choose **Security groups**.
3. From the security group list, choose the group that you want the identifier for.
4. From the **Details** tab, make a note of the identifier in the **Security Group ID** field.

Checking your data source IAM role

Make sure that your data source connector AWS Identity and Access Management IAM) role contains permissions to access your Amazon VPC.

If you use the console to create a new role for your IAM role, Amazon Q Business automatically adds the correct permissions to your IAM role on your behalf. If you use the API, or use an existing IAM role, check that your role contains permissions to access Amazon VPC. To verify that you have the right permissions, see IAM roles for data sources.

You can modify an existing data source to use a different Amazon VPC subnet. However, check your data source's IAM role and, if necessary, modify it to reflect the change for the Amazon Q Business data source connector to work properly.

Using Amazon VPC with an Amazon S3 data source

This topic describes the requirements for connecting Amazon Q Business to an Amazon Simple Storage Service through Amazon Virtual Private Cloud. It outlines the necessary prerequisites, including VPC configuration and S3 endpoint setup, to enable Amazon Q Business to access Amazon S3 buckets through a private connection.

> **Important**
>
> So that an Amazon Q Business Amazon S3 connector can access your Amazon S3 bucket, make sure that you have assigned an Amazon S3 endpoint to your virtual private cloud (VPC). For more information about configuring an Amazon Q Business Amazon S3 connector with Amazon VPC, see Using Amazon VPC with Amazon S3.

For Amazon Q Business to sync documents from your Amazon S3 bucket through Amazon VPC, you must complete the following steps:

- Set up an Amazon S3 endpoint for Amazon VPC. For more information about how to set up an Amazon S3 endpoint, see Gateway endpoints for Amazon S3 in the *AWS PrivateLink Guide*.
- (Optional) Checked your Amazon S3 bucket policies to make sure that the Amazon S3 bucket is accessible from the virtual private cloud (VPC) that you assigned to Amazon Q Business. For more information, see Controlling access from VPC endpoints with bucket policies in the *Amazon S3 User Guide*.

For more information about how to configure Amazon VPC security groups, see Security group rules in the *Amazon VPC User Guide*.

Step 3. Configure your external data source and Amazon VPC

Make sure that your external data source has the correct permissions configuration and network settings for Amazon Q Business to access it. You can find detailed instructions on how to configure your data sources in the prerequisites section of each connector page.

Also, check your Amazon VPC settings and make sure that your external data source is reachable from the subnet you will assign to Amazon Q Business. To do this, we recommend that you create an Amazon EC2 instance in the same subnet with the same security groups and test access to your data source from this Amazon EC2 instance. For more information, see Troubleshooting Amazon VPC connection.

Troubleshooting data source connectors

This section can help you fix issues with Amazon Q Business data source connectors.

Topics

- My documents were not indexed
- My synchronization job failed
- My synchronization job is incomplete
- My synchronization job succeeded but there are no indexed documents
- I am running into file format issues while syncing my data source
- I am getting an AccessDenied When Using SSL Certificate File error message
- No CloudWatch Logs for Application Using New Connector

My documents were not indexed

When you synchronize your Amazon Q Business index with a data source, you may run into issues that prevent the documents from being indexed. Indexing is a two-step process. First, the data source is checked for new and updated documents to index, and to find documents to remove from the index. Second, at the document level, each document is accessed and indexed.

An error can occur in either of these steps. Data source level errors are reported in the console in the **Sync run history** section of the data source details page. The status of the synchronization job

can be **Succeeded**, **Incomplete**, or **Failed**. You can also see the number of documents indexed and deleted during the job. If the status is **Failed**, a message is shown in the **Details** column.

Document level errors are reported in Amazon CloudWatch Logs. You can see the errors using the CloudWatch console.

You can view a document-level sync run history report in CloudWatch for your data source sync job by selecting **View Report**. A sync run history report will have details about the progress and status of each document in the sync job. It shows if a document succeeded, failed, or was skipped during the crawl, sync, and index stages. You'll also find any error messages related to failed or skipped documents. If the report doesn't show results for an in-progress sync job, the logs may not be available yet. Check back later as data is emitted to the report as events occur during the sync process.

To access your sync run history report, take the following steps:

1. Open the Amazon Q Business console.
2. From the left navigation menu, under **Enhancements**, choose **Data sources**, and then choose your data source.
3. From your data source summary page, scroll down and select the **Sync history** tab.
4. From **Sync run history**, select **Actions**.
5. From **Actions**, select **View report**. You will be redirected to the CloudWatch console where you will be able to access your report.

A sync run history records if a document was successfully indexed during ingestion, including attached ACLs and metadata, for all Amazon Q Business supported connectors.

> **Note**
>
> To learn more about generating and understanding a sync run history report, see Introducing document-level sync reports: Enhanced data sync visibility in Amazon Q Business in the *AWS Machine Learning Blog*. To learn more about analyzing data using Amazon CloudWatch, see Analyzing log data with CloudWatch Logs Insights in the *Amazon CloudWatch User Guide*.

My synchronization job failed

A synchronization job typically fails when there is a configuration error in the index or the data source. In the console, you can find the error message in the **Sync run history** section of the data source details page, under the **Details** column. Document level errors are reported in Amazon CloudWatch Logs. The error message gives information about what went wrong. The problem is usually that the index or the data source doesn't have the correct IAM permissions. The error message describes the missing permissions. Following are some of the error messages that you can receive:

```
Failed to create log group for job. Please make sure that the IAM role
provided has sufficient permissions.
```

If your index role doesn't have permissions to use CloudWatch, the data source can't create a CloudWatch log. If you get this error, you must add CloudWatch permissions to the index role.

```
Failed to access Amazon S3 file prefix (bucket name) while trying to crawl
your metadata files. Please make sure the IAM role (ARN) provided has
sufficient permissions.
```

When you're using an Amazon S3 data source, Amazon Q Business must have permissions to access the bucket that contains the documents. You need to add permissions for Amazon Q Business to read the bucket to the data source IAM role.

```
The provided IAM role (ARN) could not be assumed. Please make sure Amazon Q
Business is a trusted entity that is allowed to assume the role.
```

Amazon Q Business needs permissions to assume the index and data source IAM roles. You need to add a trust policy to the roles with permissions for the `sts:AssumeRole` action.

For the IAM policies that Amazon Q Business needs to index a data source, see IAM roles for Amazon Q Business connectors.

My synchronization job is incomplete

Jobs are generally incomplete when they have completed the data source level process but have some error during the document level process. When a job is incomplete, some of the documents might not have indexed successfully . For an Amazon S3 data source, an incomplete job is typically caused by one of the following issues:

- The metadata for one or more documents was not valid.
- When documents are submitted for indexing but at least one document was not submitted.
- When documents are submitted for deleting from the index but at least one document was not submitted.

To troubleshoot an incomplete synchronization job, look first to your CloudWatch logs.

1. From the details column, choose **View details in CloudWatch**.
2. Review the error messages to see what caused the document to fail.

My synchronization job succeeded but there are no indexed documents

Occasionally, an index synchronization job run is marked as **Succeeded**, but there are no new or updated documents indexed when you expect them. Possible reasons include the following:

- Check CloudWatch `DocumentsSubmittedForIndexingFailed` metric to see if any documents failed to synchronize. Check your CloudWatch logs for details.
- For an Amazon S3 data source, you might have given Amazon Q Business the wrong bucket name or prefix. Make sure that the S3 bucket that Amazon Q Business is using is the bucket that contains the documents to index.
- When re-indexing a document that failed to be indexed in an earlier job, Amazon Q Business won't index it unless you've changed the document or its associated metadata file.

I am running into file format issues while syncing my data source

If you run into file format issues while adding files to your data source or syncing your data source, make sure that your document types are supported by Amazon Q Business. For a list of document types supported by Amazon Q see Supported document types.

If you're using the `BatchPutDocument` API operation with plaintext files, specify `PLAIN_TEXT` as the content type.

I am getting an AccessDenied When Using SSL Certificate File error message

If you're getting an access denied error when using an SSL certificate with your data source, make sure that your IAM role has the permissions to access the SSL certificate file in its specified location.

If the certificate is encrypted with an AWS KMS key, your IAM role should also have permissions to decrypt using the AWS KMS key. For more information, see Authentication and access control for AWS KMS in the *AWS Key Management Service Developer Guide*.

No CloudWatch Logs for Application Using New Connector

I'm not seeing any CloudWatch logs for an application using a new connector.

To get the logs to display, you must call four operations before creating the connector:

1. `CreateLogGroup`: Create a log group with the name `/aws/qbusiness/${applicationId}` to be consistent with the sync run report link in the sync run history table.
2. `PutDeliverySource`: Create a delivery source with log-type set to `SYNC_JOB_LOGS`.
3. `PutDeliveryDestination`: Create a delivery destination using the log group ARN from step 1.
4. `CreateDelivery`: Create the delivery configuration linking the source and destination.

CLI Example

Replace `YOUR_APPLICATION_ID` with your actual application ID:

Step 1: Create the log group

```
aws logs create-log-group \
    --log-group-name "/aws/qbusiness/YOUR_APPLICATION_ID"
```

Step 2: Create delivery source

```
aws logs put-delivery-source \
    --name "qbusiness-sync-logs-source" \
    --log-type "SYNC_JOB_LOGS"
    --resource-arn "arn:aws:qbusiness:REGION:012345678910:application/${APP_ID}"
```

Step 3: Create delivery destination

```
aws logs put-delivery-destination \
    --name "qbusiness-sync-logs-destination" \
    --delivery-destination-configuration
 '{"destinationResourceArn":"arn:aws:logs:REGION:ACCOUNT_ID:log-group:/aws/
qbusiness/01a2c3d4-a1b2-a1b2-a1b2-01a2c3b4d5}'
```

```
    --region "region-name"
```

Step 4: Create delivery

```
aws logs create-delivery \
    --delivery-source-name "qbusiness-sync-logs-source" \
    "arn:aws:logs:region-name:012345678910:delivery-destination:qbusiness-sync-logs-
destination"
    --region "region-name"
```

Note: Update `REGION` and `ACCOUNT_ID` with your AWS region and account ID.

Verification

After completing these steps, create your connector, and run the sync job. The CloudWatch logs should now appear in the specified log group.

Managing Amazon Q Business data source resources

You can choose to manage your Amazon Q Business application environment and associated resources. To learn how to do so, see the following sections:

- Managing Amazon Q Business indices
- Managing Amazon Kendra indices
- Managing Amazon Q Business data sources
- Deleting uploaded documents

Managing Amazon Q Business indices

To manage Amazon Q Business indexes, you can take the following actions:

Actions

- Deleting an Amazon Q Business index
- Getting properties of an Amazon Q Business index
- Listing Amazon Q Business indices and retrievers
- Editing Amazon Q Business indices

Deleting an Amazon Q Business index

To delete a Amazon Q Business index, you can use the console or the DeleteIndex API operation.

If you use the console, deleting an index automatically deletes the retriever attached to it. If you use the API, you must also use the DeleteRetriever API operation to delete the Amazon Q Business retriever attached to your index.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To delete an Amazon Q Business index

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. Complete the steps to create your Amazon Q Business application.
3. In **Applications**, select the name of your application from the list of applications.
4. From the left navigation menu, choose **Data sources**.
5. From the **Data sources** page, from **Index**, select **Delete**.
6. In the dialog box that opens, type **`Confirm`** to confirm deletion, and then choose **Delete**.

   You are returned to the service console while your application environment is deleted. When the deletion process is complete, the console displays a message confirming successful deletion.

AWS CLI

To delete an Amazon Q Business index

```
aws qbusiness delete-index \
--application-id application-id \
--retriever-id index-id
```

To delete an Amazon Q Business retriever

```
aws qbusiness delete-retriever \
--application-id application-id \
--retriever-id retriever-id
```

Getting properties of an Amazon Q Business index

To get the properties of an Amazon Q Business index and retriever, you can use the console or the GetIndex and GetRetriever API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To get properties of an Amazon Q Business index and retriever

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Data sources**.
4. On the **Data sources** page, under **Index** the following settings are available:

   - **Index name** – The name of the index.
   - **Index status** – The status of your index.
   - **Index provisioning** – The number of index units provisioned for your index.
   - **Document count** – The number of documents that are attached to your index.
   - **Storage used** – The amount of storage that your index is using.
   - **Index ID** – The ID of the index attached to your retriever.
   - **Retriever ID** – The ID of the retriever that you're using.
   - **Retriever** – The retriever type that you're using.
   - **Last modified** – The time that your index was last modified.

AWS CLI

To get properties of an Amazon Q Business index and retriever

```
aws qbusiness get-index \
```

```
--application-id application-id \
--index-id index-id
```

```
aws qbusiness get-retriever \
--application-id application-id \
--retriever-id retriever-id
```

Listing Amazon Q Business indices and retrievers

To list your native Amazon Q Business indices and retrievers, you can use the console or the ListIndices API operation and the ListRetrievers API operation.

If you use the console, the list of Amazon Q Business indices and retrievers can be found within the list of data sources that you have created.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To list your Amazon Q Business indices and retrievers

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Data sources**.
4. On the **Data sources** page, a list of all indices that you have created is available.

AWS CLI

To list your Amazon Q Business indices and retrievers

```
aws qbusiness list-indices \
--application-id application-id \
--max-results maximum-result-to-display
```

```
aws qbusiness list-retrievers \
--application-id application-id \
--max-results maximum-result-to-display
```

Editing Amazon Q Business indices

To edit your Amazon Q Business index, you can use the console or the UpdateIndices API operation.

> **Note**
>
> When you update a native index, you can only update the number of storage units you provisioned for it. You can't change any other settings.

The following tab provides code examples for the AWS Management Console and AWS CLI.

Console

To update your Amazon Q Business retriever

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Data sources**.
4. In the **Data sources** page, from **Index**, select **Edit**.
5. In **Edit index**, choose to update index units provisioned from **Number of units**.
6. Select **Update** to save your changes.

AWS CLI

To update your Amazon Q Business index

```
aws qbusiness update-index \
--application-id application-id \
--index-id index-id \
--display-name display-name \
--role-arn roleArn \
```

```
--capacity-configuration IndexCapacityConfiguration="{indexId=<index-id>}"
```

Managing Amazon Kendra indices

To manage Amazon Kendra indices being used as retrievers, you can take the following actions:

Actions

- Detaching an Amazon Kendra index
- Updating an Amazon Kendra index
- Deleting an Amazon Kendra index
- Deleting an Amazon Kendra retriever
- Getting properties of an Amazon Kendra retriever
- Listing Amazon Kendra indices
- Updating an Amazon Kendra retriever

Detaching an Amazon Kendra index

To detach an Amazon Kendra index, you can use the console or the DeleteRetriever API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To detach an Amazon Kendra index

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Data sources**.
4. In the **Data sources** page, from **Index**, select **Edit**.
5. In **Edit index**, choose to update index units provisioned from **Number of units**.
6. Select **Update** to save your changes.
7. In **Applications**, choose **Actions**.
8. Choose **Detach**.
9. In the dialog box that opens, type **`confirm`** to confirm deletion, and then choose **Detach**.

You are returned to the service console while your index is detached and your retriever is deleted. When the process is complete, the console displays a message confirming successful detachment.

AWS CLI

To detach an Amazon Kendra index

```
aws qbusiness delete-retriever \
--application-id application-id \
--retriever-id retriever-id
```

Updating an Amazon Kendra index

To update an Amazon Kendra index, you can use the Amazon Q Business console or the Amazon Kendra UpdateIndex API operation.

> **Note**
>
> You can't update an Amazon Kendra Developer edition index. You can only update an Amazon Kendra Enterprise Edition index or Amazon Kendra GenAI Enterprise Edition index.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To update an Amazon Kendra index

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Data sources**.
4. In the **Data sources** page, from **Index**, select **Edit**.
5. In **Edit index**, choose between the following values to update"

- **Storage capacity** – Update your storage capacity to a value between 1-50 units. Each unit contains 20,000 documents. Index capacity must be more than the data stored in your index. If you need to, delete data and re-sync your data sources before adjusting capacity.
- **Query capacity** – Update your query capacity between 1-100 units. Each unit is 0.1 queries per second (QPS), or about 8000 queries per day.

6. Select **Update** to save your changes.

AWS CLI

To update an Amazon Kendra index

```
aws kendra update-index \
--id index-id \
--capacity-units '{"QueryCapacityUnits": 2, "StorageCapacityUnits": 1}'
```

Deleting an Amazon Kendra index

To detach an Amazon Kendra index, you can use the Amazon Kendra console or the Amazon Kendra DeleteIndex API operation.

Deleting an index removes the index and all associated data sources and document data. Deleting an index doesn't remove the original documents from your storage.

Deleting an index is an asynchronous operation. When you start deleting an index, the index status changes to `DELETING`. It remains in the `DELETING` state until all of the information related to the index is removed. Once the index is deleted, it no longer appears in the results of a call to the Amazon Kendra ListIndices API. If you call the Amazon Kendra DescribeIndex API with the deleted index's identifier, you receive and `ResourceNotFound` exception.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To delete an Amazon Kendra index

1. Sign in to the AWS Management Console and open the Amazon Kendra console at https://console.aws.amazon.com/kendra/.
2. In the navigation pane, choose **Indexes**, and then choose the index to delete.
3. Choose **Delete** to delete the selected index.

AWS CLI

To delete an Amazon Kendra index

```
aws kendra delete-index \
--id index-id
```

Deleting an Amazon Kendra retriever

To delete an Amazon Kendra retriever, you can use the console or the DeleteRetriever API operation.

If you use the console, the only ways to delete your Amazon Kendra retriever from your Amazon Q Business application environment is to detach your Amazon Kendra index from the Amazon Q Business application or delete your Amazon Q Business application environment.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI for the second scenario.

Console

To delete an Amazon Kendra retriever

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, choose **Actions**.
3. Choose **Delete**.
4. In the dialog box that opens, type **`Delete`** to confirm deletion, and then choose **Delete**.

You are returned to the service console while your application environment is deleted. When the deletion process is complete, the console displays a message confirming successful deletion.

AWS CLI

To delete an Amazon Kendra retriever

```
aws qbusiness delete-retriever \
--application-id application-id \
--retriever-id retriever-id
```

Getting properties of an Amazon Kendra retriever

To get the properties of an Amazon Kendra retriever, you can use the console or the GetRetriever API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To get the properties of an Amazon Kendra retriever

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. From the left navigation menu, choose **Data sources**.
4. On the **Data sources** page, under **Index** the following settings are available:

   - **Retriever** – The type of retriever that you're using.
   - **Document count** – The number of documents that are attached to your index.
   - **Last modified time** – The time that your index was last modified.
   - **Index ID** – The ID of the index attached to your retriever.
   - **Storage used** – The amount of storage that your index is using.

- **Index status** – The status of your index.

> **Note**
>
> You can't edit or update retriever or index settings.

AWS CLI

To get properties of an Amazon Kendra retriever

```
aws qbusiness get-retriever \
--application-id application-id \
--retriever-id retriever-id
```

Listing Amazon Kendra indices

To list your Amazon Kendra indices being used as retrievers, you can use the console or the ListRetrievers API operation.

If you use the console, the list of Amazon Kendra indices being used as retrievers can be found within the list of data sources that you have created.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To list your Amazon Q Business indices and retrievers

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Data sources**.
4. On the **Data sources** page, a list of all indices that you have created is available.

AWS CLI

To list Amazon Kendra retrivers

```
aws qbusiness list-retrievers \
--application-id application-id \
--max-results maximum-result-to-display
```

Updating an Amazon Kendra retriever

To update your Amazon Kendra retriever, you can use the UpdateRetriever API operation.

You can't update your Amazon Kendra retriever using the console.

The following tab provides code examples for the AWS CLI.

Console

This action is not supported on the console.

AWS CLI

To update an Amazon Kendra retriever

```
aws qbusiness update-retriever \
--application-id application-id \
--retriever-id retriever-id \
--display-name display-name \
--role-arn roleArn \
--configuration kendraIndexConfiguration="{indexId=<kendra-index-d>}"
```

Managing Amazon Q Business data sources

To manage data source connectors, you can perform the following actions:

Actions

- Deleting an Amazon Q Business data source connector
- Getting properties of an Amazon Q Business data source connector

- Listing Amazon Q Business data source connectors
- Updating Amazon Q Business data source connectors
- Starting data source connector sync jobs
- Stopping data source connector sync jobs
- Listing data source connector sync jobs

Deleting an Amazon Q Business data source connector

To delete an Amazon Q Business data source connector, you can use the console or the DeleteDataSource API operation .

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To delete an Amazon Q Business data source connector

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the application environment that you want to delete data sources from.
3. From the left navigation menu, select **Data sources**.
4. From the **Data sources** list, select the data source you want to delete.
5. From **Actions**, choose **Delete**.
6. In the dialog box that opens, type **`Delete`** to confirm deletion, and then choose **Delete**.

   You are returned to the service console while your data source connector is deleted. When the deletion process is complete, the console displays a message confirming successful deletion.

AWS CLI

To delete an Amazon Q Business data source connector

```
aws qbusiness delete-data-source \
--application-id application-id \
```

```
--index-id index-id \
--data-source-id data-source-id
```

Getting properties of an Amazon Q Business data source connector

To get the properties of an Amazon Q Business data source connector, you can use the GetDataSource API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To get properties of an Amazon Q Business data source connector

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the application environment you want that contains your data sources.
3. From the left navigation menu, select **Data sources**.
4. From the **Data sources** list, select the data source that you want to view details for.
5. Under **Data source details**, the following details are available:

   - **Name** – The name of your data source.
   - **Status** – The status of your data source.
   - **Last sync status** – The status of your last sync.
   - **Description** – The description that you gave to your data source.
   - **Type** – The type of data source that you're using.
   - **Last sync time** – The time that your data source was last synced.
   - **Data source ID** – The ID of your data source.
   - **IAM role ARN** – The Amazon Resource Name (ARN) of the IAM role that's associated with your data source.
   - **Current sync state** – The current sync state of your data source.

To get Amazon Q Business data source connector settings

1. Sign in to the AWS Management Console and open the Amazon Q Business console.

2. In **Applications**, select the application environment you want that contains your data sources.
3. From the left navigation menu, select **Data sources**.
4. From the **Data sources** list, select the data source you want to delete.
5. For **Data source details**, choose **Settings**.
6. For **Settings**, the following settings are available:

   - **IAM role** – The ARN of the IAM that's associated with your data source.
   - **Sync scope** – The configuration details for your data source.
   - **Sync mode** – The sync type that you chose for your data source.
   - **Sync schedule** – The sync schedule that you chose for your data source.
   - **Field mappings** – The data source document fields that you chose to map to Amazon Q Business index fields.

AWS CLI

To get Amazon Q Business data source connector properties

```
aws qbusiness get-data-source \
--application-id application-id \
--index-id index-id \
--data-source-id data-source-id
```

Listing Amazon Q Business data source connectors

To list Amazon Q Business data source connectors, you can use the console or the ListDataSources API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To list Amazon Q Business data source connectors

1. Sign in to the AWS Management Console and open the Amazon Q Business console.

2. In **Applications**, select the application environment you want that contains your data sources.
3. From the left navigation menu, select **Data sources**.
4. On the **Data sources**, under **Data sources**, a list of data sources connected to your application environment is displayed.

AWS CLI

To list Amazon Q Business data source connectors

```
aws qbusiness list-data-sources \
--application-id application-id \
--index-id index-id \
--max-results maximum-number-of-results-to-return
```

Updating Amazon Q Business data source connectors

To update your Amazon Q Business data source connectors, you can use the console or the UpdateDataSource API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To update a Amazon Q Business data source connector

Option 1

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the application environment you want to delete data sources from.
3. From the left navigation menu, select **Data sources**.
4. On the application page, from **Data sources**, select the data source that you want to edit.
5. From **Actions**, choose **Edit**.

   You are redirected to your data source configuration page to edit your existing settings.

Option 2

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the application environment you want to delete data sources from.
3. On the application page, from **Data sources**, select the data source that you want to edit.
4. On the data source page, from **Actions**, choose **Edit**.

   You are redirected to your data source configuration page to edit your existing settings.

CLI

To update your Amazon Q Business connector

```
aws qbusiness update-data-source \
--application-id application-id \
--data-source-id data-source-id \
--index-id index-id \
--configuration data-source-configuration-details \
--description description \
--display-name display-name \
--document-enrichment-configuration document-enrichment-configuration \
--role-arn roleArn \
--sync-schedule sync-schedule-information \
--vpc-configuration vpc-configuration
```

Starting data source connector sync jobs

To start Amazon Q Business data source connector sync jobs, you can use the console or the StartDataSourceSyncJobs API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To start your Amazon Q Business data source connector sync jobs

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the application environment you want to sync data sources in.

3. On the application page, from **Data sources**, select the data source that you want to sync.
4. Choose **Sync now**.

   The console displays a message confirming that your sync job has started successfully.

   > **Note**
   >
   > You can also view your sync job report in the Amazon CloudWatch console.

AWS CLI

To start your Amazon Q Business data source connector sync jobs

```
aws qbusiness start-data-source-sync-job \
--application-id application-id \
--index-id index-id \
--data-source-id data-source-id
```

Stopping data source connector sync jobs

To stop your Amazon Q Business connector sync jobs, you can use the console or the StopDataSourceSyncJobs API operation.

> **Note**
>
> You can only stop a sync job already in progress.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To stop your Amazon Q Business data source connector sync jobs

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the application environment you want to sync data sources in.

3. On the application page, from **Data sources**, select the data source that you want to stop the sync for.
4. Choose **Stop sync**.
5. In the dialog box that opens , type **Stop** to confirm your action and then select **Stop sync**.

   The console displays a message confirming that your data source sync job is being stopped.

AWS CLI

To stop your Amazon Q Business data source connector sync jobs

```
aws qbusiness stop-data-source-sync-job \
--application-id application-id \
--data-source-id data-source-id \
--index-id index-id
```

Listing data source connector sync jobs

To list Amazon Q Business data source connector sync jobs that are in progress, you can use the console or the ListDataSourceSyncJobs API operation.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To list your Amazon Q Business data source connector sync jobs

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the application environment you want that contains your data sources.
3. On the application page, from **Data sources**, select the data source that you want to view details for.
4. Under **Data source details**, choose the **Sync run history** tab.

   You will see a list of ongoing, completed, and failed sync jobs for your data sources.

CLI

To list your Amazon Q Business data source connector sync jobs

```
aws qbusiness list-data-source-sync-job \
--application-id application-id \
--data-source-id data-source-id \
--index-id index-id \
--max-results max-results-to-return
```

Deleting documents uploaded in an Amazon Q Business application

To delete documents that have been directly uploaded to an application environment, you can use the console or the BatchDeleteDocument API operation. You can delete specific documents or all documents.

The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

Console

To delete specific directly uploaded documents

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of the application environment that your uploaded files belong to.
3. From your applications page, from **Data sources**, choose **Uploaded files**.
4. In **Uploaded files**, choose **Document name**, and then select the documents that you want to delete.

   > **Note**
   >
   > You can choose up to 10 files at a time.

5. Choose **Delete files**.

You are returned to the service console while your application environment is deleted. When the deletion process is complete, the console displays a message confirming successful deletion.

AWS CLI

To delete documents

```
aws qbusiness batch-delete-document \
--application-id application-id \
--index-id index-id \
--documents documents-to-delete \
--data-source-sync-id data-source-sync-id
```

Tagging resources in Amazon Q Business

Manage your Amazon Q Business data sources, retrievers, and indexes by assigning tags. You can use tags to categorize your Amazon Q Business resources in various ways. For example, you could categorize by purpose, owner, or application, or any combination. Each tag consists of a *key* and a *value*, both of which you define.

Tags help you to do the following:

- **Identify and organize your AWS resources** – Many AWS services support tagging, so you can assign the same tag to resources in different services to indicate that the resources are related. For example, you can tag an Amazon Kendra retriever and the Amazon Q Business web experience that uses the retriever with the same tag.
- **Allocate costs** – You activate tags on the AWS Billing and Cost Management dashboard. AWS uses tags to categorize your costs and deliver a monthly cost allocation report to you. For more information, see Cost Allocation and Tagging in the *AWS Billing User Guide*.
- **Control access to your resources** – You can use tags in AWS Identity and Access Management (IAM) policies that control access to Amazon Q Business resources. To activate tag-based access control, you can attach these policies to an IAM role or IAM user. For more information, see Authorization based on tags.

You can create and manage tags using the AWS Management Console, the AWS Command Line Interface (AWS CLI), or the Amazon Q Business API.

Topics

- Using tags
- Tag restrictions

Using tags

If you're using the console, you can tag resources when you create them or add them later. You can also use the console to update or remove tags in the following ways:

Adding tags

To add Amazon Q Business tags

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From **Applications**, select the application whose resources you want to tag.
3. From the application summary page, scroll down and select **Tags**.
4. In **Tags**, from the resource you want to add tags to, select **Manage tags**.
5. In **Tags – *optional***, select **Add new tag** to add tags to your Amazon Q Business resource. Then, enter the following information for each tag:
   - **Key** – Add a key for your tag.
   - **Value - *optional*** – An optional value for your tag.
6. Select **Save**.

Removing tags

To remove tags

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From **Applications**, select the application you want to delete tags from.
3. From the application summary page, scroll down and select **Tags**.
4. In **Tags**, from the resource you want to add tags to, select **Manage tags**.
5. In **Tags – *optional***, select **Remove**.

6. Select **Save**.

Listing tags

To view a list of tags

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From **Applications**, select the application you want to delete tags from.
3. From the application summary page, scroll down and select **Tags**.
4. In **Tags**, each tagged resource will display a list of tags associated with it.

If you're using the AWS CLI or the Amazon Q Business API, use the following operations to manage tags for your resources:

- CreateApplication – Apply tags when you create an Amazon Q Business application.
- CreateWebExperience – Apply tags when you create an Amazon Q Business web experience.
- ListTagsForResource – View the tags associated with a resource.
- TagResource – Add and modify tags for a resource.
- UntagResource – Remove tags from a resource.

Tag restrictions

The following restrictions apply to tags on Amazon Q Business resources:

- Maximum number of tags – 50
- Maximum key length – 128 characters
- Maximum value length – 256 characters
- Valid characters for key and value – a–z, A–Z, space, and the following characters: _ . : / = + - and @
- Keys and values are case sensitive
- Don't use `aws:` as a prefix for keys; it's reserved for AWS use

Admin controls and guardrails in Amazon Q Business

With Amazon Q Business, you can customize your application environment to your organizational needs. Amazon Q Business offers application environment *guardrails* or *chat controls* that you can configure to control the end user chat experience.

Using the guardrails feature, you can define global controls and topic-level controls for your application environment like the following:

- Control whether end users can upload files in chat to generate responses from uploaded files.
- Control whether chat responses will be personalized to end users based on information (address and job related information) associated with them in your IAM Identity Center instance.
- Specify whether all Amazon Q Business chat responses will be generated using only enterprise data or whether your application environment can also use its underlying large language model (LLM) to generate responses when it can't find answers in your enterprise data.
- Allow Amazon Q Business to automatically orchestrate end user chat requests across any Amazon Q Business plugins and data sources you've configured.
- Allow Amazon Q Business to check its responses for hallucinations.
- Control how Amazon Q Business responds to specific topics in chat.
- Customize which users and groups Amazon Q Business topic-level controls apply to.

Topics

- Key terms for Amazon Q Business guardrails and chat controls
- Using global controls in Amazon Q Business
- Using topic-level controls in Amazon Q Business
- Managing Amazon Q Business admin controls and guardrails

Key terms for Amazon Q Business guardrails and chat controls

The following are key terms to understand guardrails in Amazon Q Business:

- **Enterprise data** – Data connected to your application environment using either an Amazon Q Business connector, direct document upload, or through an Amazon Kendra retriever.
- **Model knowledge** – The underlying knowledge outside your enterprise data that your large language model (LLM) is trained on.

- **Topic** – An admin user defined natural language topic.
- **Global controls** – application environment level controls for controlling the sources that your application environment uses to generate responses (model knowledge and enterprise data, or enterprise data only). Global controls also define and control blocked phrases within your application environment.
- **Topic controls** – Topic-specific controls to determine the web application environment's behavior when it encounters a mention of a blocked topic by an end user.
- **Rules** – An application environment behavior logic configured to manage a controlled topic for a particular group of users.

Using global controls in Amazon Q Business

You can use Amazon Q Business global controls to configure settings that apply to conversations in your application environment.

> **Note**
>
> You can't create or delete guardrail global controls. You can only update existing global controls in your application environment.

The following are the global features that you can customize:

Global controls

- Response settings
- Chat orchestration settings
- Feature settings
- Blocked phrases
- Customizing global controls

Response settings

> **Important**
>
> If you're changing response settings for an Amazon Q Business application environment created and deployed before 16 April, 2024, you need to update your web experience

service role. For information on service role permissions needed, see IAM role for an Amazon Q Business web experience. For information on how to update your web experience service role, see Updating a web experience.

Note

Displaying sample prompts to your end user using the Amazon Q Business Quick prompts feature might not work if you choose to restrict response generation to enterprise data.

When you update your application environment guardrails, you can use **Response settings** to change this behavior in the following ways:

- **Allow end users to send queries directly to the LLM** – Give end users the option to either generate LLM-only responses or only generate responses from connected data sources. If you choose to activate this option, end users will be able to toggle between generating responses from either the data sources you have connected to your application environment or use only the LLM to generate responses.

  If you choose to activate this feature for your end users, they will see the option to turn **All data sources off** or **Respond from approved sources** in their web experience. If you turn this feature off, then this option won't be available—or displayed—to end users in a web experience.

  Note

  As of Oct 31, 2024, once you have created a new Amazon Q Business application environment, this setting will be *enabled by default*, even if the Admin has not yet connected any enterprise data sources.
  For existing application environments, this setting will *remain as previously configured*.

- **Allow Amazon Q Business to fall back to LLM knowledge** – Allow Amazon Q Business to use its LLM knowledge to generate responses when it can't find responses from your connected data sources. If you choose to activate this mode, and haven't given your end users the option to choose how responses are generated, your application environment will default to producing responses using the LLM when it can't find information in your data sources.

- **Personalize responses** – Allow Amazon Q Business to customize chat responses to end users using metadata associated with them—specifically address and job related information—in your IAM Identity Center instance.

  You must have already added this information in IAM Identity Center for response personalization to work as intended. For more information on how to configure your IAM Identity Center instance for personalization see Personalizing chat responses.
- **Enable hallucination mitigation** – Allow Amazon Q Business to check the chat responses it generates for hallucinations. If a hallucination is detected with high confidence, Amazon Q Business corrects the inconsistencies in its response real-time during chat and generates a new, edited message.

  The hallucination mitigation feature is only available for retrieval augmented generation (RAG) responses from data connected to the application—either through connected data sources, or files uploaded during chat (up to 100,000 characters).

  Hallucination mitigation isn't supported for the following use cases:

  - Applications where chat orchestration is enabled.
  - Plugin workflows.
  - Responses generated from tabular data, or from transcripts of images, audio and video. Hallucination mitigation applies only to responses generated from textual data.

> **Important**
>
> Activating hallucination mitigation will increase chat response latency.

Global controls apply to all supported conversation interactions, except when it conflicts with a specific topic-level control. In that case, a topic-level control takes precedence.

Chat orchestration settings

You can use **Chat orchestration settings** to automatically manage chat requests across configured plugins and data sources in your Amazon Q Business application. If you activate chat orchestration, Amazon Q Business automatically routes chat requests to plugins, integrating enterprise data and relevant actions within a single chat response. Users get direct responses without manual plugin selection.

> **Note**
>
> Chat orchestration is optimized to work for English language content. For more details on language support in Amazon Q Business, see Supported languages. Additionally, the hallucination mitigation feature won't work if chat orchestration controls are enabled for your application.

The following are the key features of chat orchestration:

- **Unified response integration** – Lets Amazon Q Business combine its retrieval augmented generation (RAG) workflow with plugin actions. This allows Amazon Q Business to provide comprehensive answers in natural language during conversations. For example, Amazon Q Business can explain paid time-off (PTO) policy from company data and create a time-off request at the same time.
- **Intelligent action detection** – Allows Amazon Q Business to automatically identify read-only chat requests (like checking ticket counts) and write actions (like creating a ticket) and present forms for user validation.
- **Smart plugin management** – Allows Amazon Q Business to automatically select appropriate plugins without manual user selection while managing multiple complex plugin interactions.
- **User driven experience** – Enables Amazon Q Business to ask for user clarification when multiple actions are possible, validating actions before taking them, and guiding the user through the information needed to perform an action.

If you deactivate chat orchestration, Amazon Q Business won't relay queries across data sources and plugins. Users must manually select to use plugin mode to invoke a plugin action from chat.

If you're using an Quick plugin (fully-integrated with Amazon Q Business and not available for manual selection by users during chat), activating chat orchestration affects its behavior. With chat orchestration enabled, an Quick plugin only activates if:

- No other plugin actions (read or write requests requiring additional end user input through forms) are detected, or, in progress.
- No end user authentication requests are pending.

Feature settings

You can control whether end users can upload files during chat to ask questions based on the uploaded document. By default, your application environment allows your end users to directly upload files in chat.

You can also choose whether to allow end users in a web experience to create and use Amazon Q Apps. Amazon Q Apps relies on LLM knowledge to work.

Blocked phrases

You can define blocked phrases for your application environment. Amazon Q Business ensures that chat responses don't include these words. You can choose up to 20 words.

Additionally, you can optionally configure a custom message to be displayed to your end users in response to any mention of blocked phrases during chat. You can use this message to inform them that word is blocked and provide them with further guidance on next steps.

By default, your application environment doesn't define any blocked words. You can choose to add these words when you edit and update your global control guardrails.

Customizing global controls

When you create an Amazon Q Business application environment, it's assigned the following default global controls:

- An option to generate responses from either enterprise data or LLMs.
- Response personalization is activated.
- Automatic orchestration of end user chat requests across any Amazon Q Business plugins and data sources you've configured.
- File upload by end user during chat is activated.
- Q Apps creation is activated.
- Hallucination mitigation is deactivated. To turn hallucination mitigation on, you must first deactivate chat orchestration.

To update global topic controls for your web experience chat, you can use the AWS Management Console or the UpdateChatControlsConfiguration API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

> **Note**
>
> You can't create or delete guardrail global controls. You can only update existing global controls in your application environment.

Console

To update a global control guardrail

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. From the left navigation menu, choose **Enhancements**, and then choose **Guardrails**.
4. In **Guardrails**, from **Global controls**, choose **Edit**.
5. In **Application guardrails**, do the following:

   - For **Response settings** do the following:
     - **Allow end users to send queries directly to the LLM** – If you choose to activate this option, end users will be able to toggle between generating responses from either the data sources you have connected to your application environment or use only the LLM to generate responses.

       > **Note**
       >
       > If you choose to enable this option, your end users will have the option to generate LLM-only responses even if you don't allow Amazon Q to user LLM knowledge to generate responses.

       For more information, see Using global controls in Amazon Q Business.
     - **Allow Amazon Q Business to fall back to LLM knowledge** – Choose this option if you want to generate responses from your application environment's LLM world knowledge when it can't find information in your connected data sources. The default is to restrict responses to enterprise data. For more information, see Using global controls in Amazon Q Business.

- **Personalize responses** – Allow Amazon Q Business to customize chat responses to end users using metadata associated with them—specifically address and job related information—in your IAM Identity Center instance.

  > **Note**
  >
  > You must have already added this information in IAM Identity Center for response personalization to work as intended. For more information on how to configure your IAM Identity Center instance for personalization see Personalizing chat responses.

- **Enable hallucination mitigation** – Allow Amazon Q Business to check the chat responses it generates for hallucinations. If a hallucination is detected with high confidence, Amazon Q Business corrects the inconsistencies in its response real-time during chat and generates a new, edited message.

  > **Note**
  >
  > You must deactivate **Chat orchestration settings** before you can activate hallucination mitigation.

6. For **Chat orchestration settings**, activate to automatically manage chat requests across configured plugins and data sources in your Amazon Q Business application. If you activate chat orchestration, Amazon Q Business automatically routes chat requests to plugins, integrating enterprise data and relevant actions within a single chat response. Users get direct responses without manual plugin selection.

   > **Note**
   >
   > You must deactivate **Enable hallucination mitigation** before you can activate chat orchestration.

7. For **Feature settings**, choose whether your end users will be allowed to upload files directly in chat to ask questions based on file content and whether Amazon Q Apps will be enabled for your application environment.

8.
   - For **Blocked words** – Define blocked words for the application environment. The application environment will not respond to questions that contain these words or mention them in any responses.
   - For **Messaging shown for blocked words** – Choose to create a custom response for your end users informing them of blocked word usage and any next steps to take.
9. Choose **Save**.

AWS CLI

To update a global control guardrail

```
aws qbusiness update-chat-controls-configuration \
--application-id application-id \
--blocked-phrases-configuration-update '{"blockedPhrasesToCreateOrUpdate":["example
 phrase 1", "example phrase 2"],"blockedPhrasesToDelete":["example phrase 1",
 "example phrase 2"],"systemMessageOverride":"user facing message when blocked
 phrase encountered"}' \
--client-token clientToken \
--response-scope ENTERPRISE_CONTENT_ONLY | EXTENDED_KNOWLEDGE_ENABLED \
--creator-mode-configuration creatorModeControl=ENABLED | DISABLED \
--orchestration-configuration orchestrationControl=ENABLED | DISABLED \
--hallucination-reduction-configuration '{"hallucinationReductionControl": "ENABLED"
 | "DISABLED"}'
```

Using topic-level controls in Amazon Q Business

You can use topic-level controls to specify special topics within your application environment. You can configure rules to customize how Amazon Q Business should respond when a chat message matches a special topic. To streamline your application environment's response, you provide a name and a short description for how the large language model (LLM) should respond based on the topic-specific guardrail you're building. You can configure up to 2 topic-level controls.

Topic-level controls provide fine-grained customization for your application environment. For example, you can define a global control guardrail that allows your application environment to generate responses using model knowledge. You can also use a content retrieval rule to limit response generation for specific topics to enterprise content.

The following are the topic-level guardrails that you can customize:

Topic level guardrails

- LLM prompt control
- Application behavior rules
- Creating topic controls

LLM prompt control

You can add up to 5 representative messages that you expect end users to submit about this topic. You can also configure natural language descriptions to define the boundaries of the topic. Amazon Q Business uses these messages to check the responses that it generates for restricted content.

Application behavior rules

You can configure behavior rules that control how Amazon Q Business responds for each special topic that you specify.

> **Note**
>
> You can specify up to 5 rules per special topic.

Rules

- Answer using enterprise data
- Blocking special topics

Answer using enterprise data

When your application environment encounters a special topic, you can choose to allow it to answer from your enterprise data. If you allow responses from your enterprise data, you can further restrict which data sources in your application environment that your responses are generated from.

You can also choose to specify the specific users or groups within your application environment to apply this rule to, using either an inclusion logic or an exclusion logic. You can't use both kinds of logic at once. If a user is a member of a group with conflicting rules defined, Amazon Q Business will apply the more restrictive rule to that user.

Blocking special topics

When your application environment encounters a special topic, you can choose to block responses completely. If you do so, you can configure a custom message to display to your end users in response to any mention of blocked topics during chat. Use this message to inform your end users that the topic is blocked and provide them with further guidance on next steps.

You can also choose to specify the specific groups within your application environment to apply this rule to, using either an inclusion logic or an exclusion logic. You can't use both kinds of logic at once. If a user is a member of a group with conflicting rules defined, Amazon Q Business will apply the more restrictive rule to that user.

Not specifying an inclusion or exclusion logic will result in the rule being applied to all users.

> **Note**
>
> User level rule creation is not currently supported for the following IAM Identity Provider access management methods: SAML and OIDC.

Creating topic controls

To create an Amazon Q Business topic-level control for your web experience chat, you can use AWS Management Console or the UpdateChatControlConfiguration operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To create a topic control

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. From the left navigation menu, choose **Enhancements**, and then choose **Guardrails**.
4. For **Guardrails**, from **Topic specific controls**, choose **Create topic control**.
5. For **Create topic specific controls**, enter the following information:

   - **Name** – Enter a name for your topic-specific control.

- **Description** – A natural language description for your topic control configuration. Use this to help the LLM better identify queries associated with the topic control you're configuring.

6. For **Example chat messages**, enter representative phrases that you expect a user to type to invoke this topic. You can add up to 5 messages.
7. (Optional) To configure a rule, choose **Add new rule**.
8. For **Rule 1**, enter the following information:

   - In **Behavior in response to guardrail**, for **Behavior** – Choose how Amazon Q Business will respond to blocked topics: **Answer using enterprise data** or **Block completely**.
   - If you choose **Block completely** – Choose to include a custom message to inform your end user of restricted topics from chat and suggest follow up actions.
   - If you choose **Answer using enterprise data**, **Data source requirements** – Choose data sources that Amazon Q Business will use to generate responses.

9. For **User handling**, specify the users or groups that this topic control rule applies to and any users or groups that are exempt from this rule.
10. Choose **Save**.

AWS CLI

To create a topic control

```
aws qbusiness update-chat-controls-configuration \
--application-id application-id \
--client-token clientToken \
--topic-configurations-to-create-or-update
 '[{"name":"name","description":"description","exampleChatMessages":
["message1", "message2"],"rules":[{"includedUsersAndGroups":{"userIds":
["userId1","userId2"],"userGroups":["userGroup1","userGroup2"]},"ruleType":
 "CONTENT_BLOCKER_RULE","ruleConfiguration":{"contentBlockerRule":
{"systemMessageOverride":"custom_message"}}},{"excludedUsersAndGroups":
{"userIds":["id1", "id2"],"userGroups":["group1", "group2"]}, "ruleType":
 "CONTENT_RETRIEVAL_RULE", "ruleConfiguration":{"contentRetrievalRule":
{"eligibleDataSources":[{"indexId":"index-id1","dataSourceId":"data-source-id1"},
{"indexId":"index-id2","dataSourceId":"data-source-id2"}]}}}]}]' \
--topic-configurations-to-delete '{"name":"existing-topic-name"}'
```

> **Note**
>
> The user IDs you add to configure topic controls must already exist in your Identity Provider (IdP). You are responsible for validating any user groups you add.

Managing Amazon Q Business admin controls and guardrails

To manage Amazon Q Business admin controls and guardrails, you can take the following actions:

> **Note**
>
> You can't create or delete guardrail global controls. You can only update existing global controls in your application environment.

Actions

- Deleting topic controls
- Getting topic control properties

Deleting topic controls

To delete configured chat controls, you can use AWS Management Console or the DeleteChatControlsConfiguration API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To delete topic controls

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. From the left navigation menu, choose **Enhancements**, and then choose **Guardrails**.
4. In **Guardrails**, from **Topic specific controls**, choose the topic control you want to delete, and then choose **Delete**.
5. In the dialog box, type **`delete`** to confirm your action.

The console displays a successful deletion message when the plugin deletion process is finished.

AWS CLI

To delete a topic specific control

```
aws qbusiness delete-chat-controls-configuration \
--application-id application-id
```

Getting topic control properties

To get the details of Amazon Q Business topic controls, you can use either the AWS Management Console or the GetChatControlsConfiguration API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To get configured details for admin controls and guardrails

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the Amazon Q Business console, in **Applications**, select the name of your application environment from the list of applications.
3. From the left navigation menu, choose **Enhancements**, and then choose **Admin controls and guardrails**.

   You will find the details of your configured **Global controls** and **Topic specific controls** on the page.

AWS CLI

To get admin controls and guardrails details

```
aws qbusiness get-chat-control-configuration \
--application-id application-id
```

Customizing responses in Amazon Q Business

Response customization in Amazon Q Business allows you to control how the Amazon Q Business generates and formats responses to user queries. By configuring response settings, you can ensure that Amazon Q Business communicates in a way that matches your organization's voice, style, and communication preferences.

With response customization, you can:

- Define the length and level of detail in responses
- Set the appropriate tone and formality level
- Specify formatting preferences such as bullet points or paragraphs
- Tailor responses for different audience types
- Create a consistent identity and voice for your Amazon Q Business application

> **Note**
>
> You can't use response customization to change Amazon Q Business chat orchestration settings, or citation generation and formatting.

Response customization settings

When you create an Amazon Q Business application, Amazon Q Business applies its default response settings to your application. You can choose to customize these default settings to meet your particular use case.

When configuring custom response settings, keep the following best practices in mind:

- Keep instructions clear and specific
- Avoid contradictory directives
- Use positive instructions whenever possible
- Use negative prompts only to prevent undesirable output or biased responses
- Maintain consistency across related instructions
- Add relevant, diverse, and real-world scenario-based examples
- Don't include sensitive or personally identifiable information (PII)

Note

- Response customization settings don't overwrite any admin controls and guardrails already applied to your application.
- In cases where custom response settings can't be applied to a specific response, Amazon Q Business will apply it's default response settings.
- To optimize performance and accuracy, Amazon Q Business may pre-process custom prompts before using them to generate responses.

When customizing responses in Amazon Q Business, you can configure the following settings:

Response customization settings

- Identity
- Perspective
- Target audience
- Output style
- Tone
- Response length
- Custom instructions

Identity

Define the persona or identity that Amazon Q Business should adopt when responding to users. This allows you to customize the assistant's character, role, or representation within your organization.

When configuring identity, consider the following best practices:

- Keep character/persona descriptions consistent
- Define clear boundaries of expertise
- Specify relevant background information
- Don't create harmful or discriminatory personas
- Avoid mixing multiple conflicting identities

- Don't impersonate real individuals or protected entities

Perspective

Choose the point of view from which Amazon Q Business generates responses, such as first-person, second-person, or third-person perspective. This affects how information is presented to users and can help establish the right relationship between the assistant and users.

When configuring perspective, consider the following best practices:

- Define clear view points or approaches
- Specify professional or industry perspectives, when relevant
- Maintain ethical boundaries
- Don't request biased or discriminatory perspectives
- Avoid mixing conflicting viewpoints
- Don't ask for harmful or dangerous perspectives

Target audience

Define the intended audience for responses, allowing Amazon Q Business to tailor its language, terminology, and explanations appropriately. You can configure responses for technical experts, general users, or specific custom roles within your organization.

When configuring target audience, consider the following best practices:

- Clearly define intended audience
- Specify technical level, if relevant
- Include age-appropriate considerations
- Don't define inappropriate audiences
- Don't mix incompatible audience levels

Output style

Specify the formatting and structural style of responses, such as bullet points, paragraphs, step-by-step instructions, or other organizational formats that enhance readability and comprehension.

When configuring output style, consider the following best practices:

- Specify preferred formatting clearly
- Define structure preferences
- Include any special markers or indicators needed
- Don't mix incompatible formatting styles
- Don't request harmful or inappropriate content
- Ensure your prompt instructions respect safety and security

Tone

Control the emotional tone and communication style of responses—such as formal, casual, technical, friendly, or professional—to align with your organization's communication standards and user expectations.

When configuring tone, consider the following best practices:

- Specify clear mood/attitude
- Match tone to purpose and audience
- Maintain consistency
- Don't mix conflicting tones
- Don't ignore context when setting tone
- Don't request inappropriate or offensive tones

Response length

Control whether responses are concise and brief or more detailed and comprehensive. This setting helps ensure that users receive information at the appropriate level of detail for their needs.

When configuring response length, consider the following best practices:

- Specify clear length preferences (brief, detailed, for example)
- Define word/character limits if needed
- Match content type (social media post, for example) to response length (150 words, for example)
- Don't give contradicting length requirements
- Don't request unreasonable lengths

Custom instructions

Provide specific guidance for how Amazon Q Business should respond in particular scenarios or to certain types of queries, enabling fine-grained control over response generation.

When configuring custom instructions, consider the following best practices:

- Provide clear, actionable directives
- Keep instructions focused on one aspect at a time
- Use specific examples when needed
- Avoid contradicting instructions (For example: "Be formal and casual")
- Don't include harmful or toxic content
- Don't add too many instructions

Managing response configurations

When you create an Amazon Q Business application, Amazon Q Business applies default response settings to it. You can customize responses for a Amazon Q Business application using the AWS Management Console and the API.

Response customization management

- Creating custom response settings
- Editing response customization settings
- Deleting existing response customization settings
- Listing response customization settings

Creating custom response settings

You can customize Amazon Q Business responses using the AWS Management Console or the CreateChatResponseConfiguration API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

> **Note**
>
> To optimize performance and accuracy, Amazon Q Business may pre-process custom prompts before using them to generate responses.

Console

To customize responses

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In the navigation pane, choose **Applications**, and then select your application.
3. Choose **Enhancements** from the navigation menu, and then select **Response customization**.
4. From **Response customization**, choose **Edit**.
5. In **Edit response settings**, in **Persona**, do the following:
    a. For **Define assistant's identity**, define the persona for your assistant. You can choose between selecting the default Amazon Q Business identity or defining a custom identity for your assistant.
    b. For **Describe assistant's perspective**, select the point of view for assistant responses. You can choose between selecting the default Amazon Q Business perspective or defining a custom role and perspective for your assistant.
    c. For **Describe assistant's audience**, specify the intended audience for responses. You can choose between selecting the default Amazon Q Business perspective or defining a specific audience that your assistant will be interacting with.
6. In **Edit response settings**, in **Response preference**, do the following:
    a. For **Set default response style**, choose the formatting style for responses. You can choose between selecting the default Amazon Q Business response style or defining a custom response style for your assistant.
    b. For **Set default response tone**, select the communication style for responses. You can choose between selecting the default Amazon Q Business response tone or defining a custom response tone for your assistant.
    c. For **Set response length**, choose the appropriate level of detail for responses. You can choose between selecting the default Amazon Q Business response length or defining a custom response length for your assistant.
7. For **Additional instructions – *Optional***, enter any other specific guidance for response generation.
8. Choose **Save** to save your configuration.

AWS CLI

To create a response configuration

```
aws qbusiness create-chat-response-configuration \
--application-id application-id \
--display-name configuration-name \
--client-token client-token \
--response-configurations '[
  {
    "instructionCollection": {
      "responseLength": "DETAILED",
      "targetAudience": "TECHNICAL_EXPERTS",
      "perspective": "FIRST_PERSON",
      "outputStyle": "BULLET_POINTS",
      "identity": "ASSISTANT",
      "tone": "PROFESSIONAL",
      "customInstructions": "Provide detailed technical explanations with code
 examples when appropriate.",
      "examples": "Example 1: When asked about Lambda, explain the service, its key
 features, and include a simple code example."
    }
  }
]'
```

Editing response customization settings

You can edit an existing response configuration using the AWS Management Console or the UpdateChatResponseConfiguration API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To edit response customization settings

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In the navigation pane, choose **Applications**, and then select your application.
3. Choose **Enhancements** from the navigation menu, and then select **Response customization**.
4. From **Response customization**, choose **Edit**.

5. In **Edit response settings**, modify the configuration settings as needed.

> **Note**
>
> You can also reset an all existing customizations to the default used by Amazon Q Business. To do so, select **Reset to defaults**.

6. Choose **Save** to apply your changes.

AWS CLI

To update a response configuration

```
aws qbusiness update-chat-response-configuration \
--application-id application-id \
--chat-response-configuration-id configuration-id \
--display-name updated-name \
--client-token client-token \
--response-configurations '[
  {
    "instructionCollection": {
      "responseLength": "CONCISE",
      "targetAudience": "GENERAL_USERS",
      "perspective": "SECOND_PERSON",
      "outputStyle": "PARAGRAPHS",
      "identity": "EXPERT",
      "tone": "FRIENDLY",
      "customInstructions": "Provide clear, concise explanations suitable for
 general users.",
      "examples": "Example 1: When asked about Lambda, provide a brief overview in
 simple terms."
    }
  }
]'
```

Deleting existing response customization settings

You can delete configured response customizations using the DeleteChatResponseConfiguration API operation. If you're using the AWS Management Console, you can't reset the response

customizations you have configured to default. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To reset response customization settings to default

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In the navigation pane, choose **Applications**, and then select your application.
3. Choose **Enhancements** from the navigation menu, and then select **Response customization**.
4. From **Response customization**, choose **Edit**.
5. In **Edit response settings**, select **Reset to defaults**. This resets all existing customizations to the default used by Amazon Q Business.
6. Choose **Save** to apply your changes.

AWS CLI

To delete a response configuration

```
aws qbusiness delete-chat-response-configuration \
--application-id application-id \
--chat-response-configuration-id configuration-id
```

Listing response customization settings

You can list all available response configurations for an application using the AWS Management Console or the GetChatResponseConfiguration and ListChatResponseConfigurations API operations. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To list response customization settings

1. Sign in to the AWS Management Console and open the Amazon Q Business console.

2. In the navigation pane, choose **Applications**, and then select your application.
3. Choose **Enhancements** from the navigation menu, and then select **Response customization**. You'll see a list of existing response customizations displayed on the page.

AWS CLI

To list response configurations

```
aws qbusiness get-chat-response-configuration \
--application-id application-id \
--chat-response-configuration-id chat-response-configuration-id
```

```
aws qbusiness list-chat-response-configurations \
--application-id application-id \
--max-results 10 \
--next-token next-token
```

Share your enterprise data with data accessors using Amazon Q index

The Amazon Q Business data accessors feature allows you to securely share your enterprise data with verified independent software vendors (ISVs) using Amazon Q. This feature allows ISVs to retrieve relevant content from your Amazon Q index, enhancing their applications with your organization's knowledge. By granting controlled access to your data, you can leverage third-party tools while maintaining security and data access compliance.

DataAccessor supports two types of authorization patterns to access ISVs end user data on Amazon Q:

- Authorization Code

  AWS IAM Identity Center supports OAuth 2.0 authorization code flows using the Proof Key for Code Exchange (PKCE) standard. This provides AWS applications, such as Amazon Q Business, a simple and safe way to authenticate users and obtain their consent to access Amazon Q Business resources from desktops and mobile devices with web browsers.

- Trusted token issuer/App level authentication
  - A trusted token issuer is an OAuth 2.0 authorization server that creates signed tokens. These tokens authorize applications that initiate requests (requesting applications) for access to AWS managed applications (receiving applications).
  - Consideration for granting an ISV with trusted token issuer based authorization

This topic discusses how an Amazon Q Business administrator can connect to one of the supported data accessors.

Topics

- A list of verified software providers who are data accessors
- Prerequisites
- Add a data accessor (ISV) to connect to your Amazon Q index
- Completing the process to add a data accessor
- Deleting or removing a data accessor's access from your Amazon Q index

A list of verified software providers who are data accessors

The following are the *verified* independent software vendors (ISVs) that are data accessors.

- **Asana** — Data accessor configuration registration page
- **Miro**
- **Zoom** — Data accessor configuration registration page
- **PagerDuty** — Data accessor configuration registration page
- **Kore.ai** — Data accessor configuration registration page
- **Karini AI** — Data accessor configuration registration page
- **Revinova**
- **Planview** (available in `us-west-2` only) — Data accessor configuration registration page
- **Amplience** — Data accessor configuration registration page
- **Saviynt**
- **Webex by CISCO** — Data accessor configuration registration page
- **Fireflies.ai**

- **SUSE Rancher for Amazon Web Services**
- **CXone Mpower**

Prerequisites

To add an ISV as a data accessor, complete the following prerequisites:

1. Get started with Amazon Q Business
2. Create an Identity and Access Management (IAM) Identity Center-integrated application (IAM Federated application environments are not supported at this time).
3. Set up the retriever and connect your data sources. For a complete list of data source connectors (see supported connectors). You need the relevant credentials from each connector that you want to retrieve data from. For more information, see Creating a retriever for an Amazon Q Business application environment and Connecting Amazon Q Business data sources.
4. If you are using a customer managed key in your Amazon Q Business Application, you must set your key policy to allow the ISV principal access to the KMS key with the following policy:

   JSON

```
{
    "Version":"2012-10-17",
    "Id": "isv-key-consolepolicy",
    "Statement": [
        {
            "Sid": "EnableIAMUserPermissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/isv-role"
            },
            "Action": "kms:Decrypt",
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "qbusiness.us-east-1.amazonaws.com"
                    ]
                }
            }
        }
```

```
    ]
}
```

Add a data accessor (ISV) to connect to your Amazon Q index

After setting up your application environment and connecting your data source(s), Amazon Q Business begins indexing your enterprise data. You still need to add the software providers (ISVs) as a data accessor and provide configuration details to the ISV to retrieve content from your Amazon Q index. By adding a data accessor, you grant their AWS account to access the Amazon Q index via the `SearchRelevantContent` API operation.

You can grant data accessor permissions to your Amazon Q index using either the Amazon Q Business console or the Amazon Q Business API. The following procedures show how to do this using the Amazon Q Business console or the AWS CLI.

> **Important**
>
> You must provide the setup details generated when adding your ISV as a data accessor to your ISV so they can access your Amazon Q index. You can find this information at any time in the **Information for data accessor** tab in the **data accessor details** page which is accessed by choosing the accessor **Name** from the **Data accessors** table on the **Data accessors** page.

The following tabs provide the instructions for how to retrieve your `Tenant ID` for each ISV. In data accessors, the `External Id` is the same as `Tenant Id`.

Asana

In Asana, the Tenant ID in Amazon Q Business Data Accessor is called the `domain ID`. You can use the following instructions to retrieve the Asana Tenant ID

1. Choose your account profile picture and select Admin Console.
2. Select Settings.
3. Scroll to Domain Settings to retrieve the Tenant ID.

PagerDuty

In PagerDuty, the tenant ID in Amazon Q Business Data Accessor is called the tenant ID. You can use the following instructions to retrieve the PagerDuty the Tenant ID

1. Select the User Icon.
2. Select Account Settings.
3. Select the PagerDuty Advance tab.
4. Toggle Enable Amazon Q to the on position.
5. The PagerDuty Tenant ID is now available from the Amazon Q Business Configuration Values modal.

Kore.ai (AIforWork)

In AIforWork, the Tenant ID is displayed directly in the setup form. You can use the following instructions to retrieve the Kore.ai Tenant ID:

1. Navigate to AIforWork platform.
2. When setting up an Enterprise Knowledge or Search Agent, choose **Q for Business**.
3. In the setup form that opens, the Tenant ID is displayed and ready to copy.

Revinova

The Portal ID in Revinova is the Tenant ID for Amazon Q Business Data Accessor. You can use the instructions below to retrieve the Portal ID from Revinova.

1. Log in to the admin console.
2. Navigate to the portals dashboard using the **Portals** menu under the settings menu collection.
3. In the portal's grid, hover on the header of any of the columns and click on the hamburger menu shown in the column to open the column options context menu.
4. Click on the grid icon available on the top right corner of the column options context menu.
5. Select **ID** from the list of columns available for display, and it will show the portal IDs in the grid.
6. You can get the ID for the portal from the corresponding row.

Planview

Your Planview Tenant ID is a unique identifier in UUID/GUID format (e.g., 12345678-1234-1234-1234-123456789abc).

For Planview, the Tenant ID information can be found in their integration documentation. You can use the following resource to retrieve the Tenant ID for Planview Viz integration with Amazon Q Business.

1. Refer to the Planview Amazon Q Business Integration FAQ for detailed instructions on retrieving your Tenant ID.

> **Note**
>
> Planview data accessor is only available in the `us-west-2` region.

Amplience

For Amplience, the Tenant ID is the Hub ID. You can use the following instructions to retrieve the Amplience Tenant ID.

1. Within Amplience Dynamic Content, switch into the Hub you wish to connect.
2. Select the settings icon in the top right corner and select the **Properties** menu item.
3. The Hub ID will be displayed with a copy to clipboard option.

Saviynt

For Saviynt, the Tenant ID is the FQDN from the Saviynt Console. You can use the following instructions to retrieve the Saviynt FQDN.

The URL will look similar to this example https://ispm-dev.saviyntcloud.com/ and the tenant id from this example will be "ispm-dev.saviyntcloud.com"

Webex by CISCO

In Webex, the tenant ID in Amazon Q Business Data Accessor is called the Organization ID. You can use the following instructions to retrieve the Webex Tenant ID.

1. Login in Cisco Control Hub.

2. Go to Account->Info page.

3. Copy the Organization ID.

Fireflies.ai

When prompted for Tenant ID, please enter Team ID

Miro

For Miro, the Tenant ID is Organization ID. Organization admins can navigate to the 'Organization profile' page and get the id from the address bar.

SUSE Rancher for Amazon Web Services

For SUSE Rancher for Amazon Web Services, the Tenant ID is tenant-uid. The tenant-uid can be found within the application in the about info in the top right of the screen.

CXone Mpower

For CXone Mpower, the Tenant ID required for the Amazon Q Business Data Accessor is displayed on your My Profile page. To access this page,

- In the upper-right corner of any page in the platform, click your initials.

- Select My Profile from the menu.

- On the General tab of the My Profile page, locate your Tenant ID.

Topics

- Add a data accessor using the console
- Adding a data accessor using the AWS CLI

Add a data accessor using the console

Prerequisite for both Auth code and TTI configurations.

`tenantID`

The `tenantID` is a unique identifier for your application tenant. Each application might have different terms for a tenant such as Workspace ID for Slack or Domain ID for Asana. You can review the Prerequisites page to see how to retrieve the `TenantId` for your application.

1. Sign in to the Amazon Q Business console.
2. Choose **Applications**, then select the name of your application environment from the list.
3. From the left navigation, choose **Data accessors**.
4. Choose the authentication method, **Auth Code** or **Trusted Token Issuer (TTI)** from the list of options.
5. Choose from the list of approved and supported data accessors (ISVs).
6. Choose a **Name** for this data accessor's instance, for example **`<your application-name>-<accessor-name>`**.

   If you chose TTI, follow these steps to configure the authentication:

   1. Enter your **External Id (same as Tenant Id)**, **Trust Token Issuer name**, **Identity provider attribute**, and **IAM Identity Center attribute**.
   2. Select, **Create trusted token issuer**.
7. Choose **Data source access** between **Allow all** or **Allow specific data sources** depending on whether you want to provide the ISV access to all or certain data sources from your Amazon Q index.
8. Choose the end **User access**. These are the end users that will connect with and use the Amazon Q index data from within the ISV's application. You can choose between all users that have access to the Amazon Q Business application environment or a subset of users and groups that you can define.
9. Choose **Add data accessor** to confirm your choices and add the data accessor.

   > **Note**
   >
   > You must provide the setup details generated when adding your ISV as a data accessor to your ISV so they can access your Amazon Q index. You can find this information at any time in the **Information for data accessor** tab in the **data accessor details** page which is accessed by choosing the accessor **Name** from the **Data accessors** table on the **Data accessors** page.
10. The data accessor you have added will now appear as an entry in the table on the main **Data accessors** page.

Adding a data accessor using the AWS CLI

In order to add an ISV as a data accessor you will need to call 3 APIs. First, the `CreateDataAccessor` API operation will create a data accessor and associate your application ID. `AssociatePolicy` operation API to attach the resource based policy for cross account API calls. Finally, you will set your user assignment for the Identity and Access Management (IAM) Identity Data Center (IDC) application environment with `PutApplicationAssignment` API. For granular user access control, use the Amazon Q Business console.

Prerequisite for both Auth code and TTI configurations.

`tenantID`

The `tenantID` is a unique identifier for your application tenant. Each application might have different terms for a tenant such as Workspace ID for Slack or Domain ID for Asana. You can review the Prerequisites page to see how to retrieve the `TenantId` for your application.

ISV data accessor principal role ARNs for the CreateDataAccessor API

The following are the `principal` role ARNs for the supported ISVs:

- Asana — `arn:aws:iam::865993441991:role/autogen_role_customer-byoq-data-accessor_customer_q_biz_d-217f4f`
- Miro — `arn:aws:iam::380983552397:role/AwsQBusinessMiroRetriever`
- Zoom — `arn:aws:iam::796973485215:role/zoom-ai-amazon-q-business-retrieval-role`
- PagerDuty — `arn:aws:iam::748801462010:role/terraform/pagerduty-isv-qretriever-dataaccessor-role`
- Kore.ai — `arn:aws:iam::452460288037:role/Q4BTrustPolicyRole`
- Karini AI — `arn:aws:iam::891377073540:role/Karini-AmazonQ-Data-Accessor-Role`
- Revinova — `arn:aws:iam::833755663361:role/revinova_q_business_isv_role`
- Planview (available in `us-west-2` only) — `arn:aws:iam::431569694887:role/ep-copilot-production-us-west-2-q-index-role-tti`
- Amplience — `arn:aws:iam::123645302184:role/q-index-isv-role`
- Saviynt — `arn:aws:iam::249469748895:role/ispm-isv-qindex`
- Webex by CISCO — `arn:aws:iam::973559386291:role/WebexSuit-QIndex-role-prod`
- Fireflies.ai — `arn:aws:iam::466023587921:role/awsQAccessorRole`

- SUSE Rancher for Amazon Web Services — `arn:aws:iam::940482441539:role/mcm-q-data-accessor`
- CXone Mpower — `arn:aws:iam::765956972205:role/nice_csa_kh_qindex_retriever_trust_role`

Action configuration (JSON) example for the CreateDataAccessor API

- `action` — Only `qbusiness:SearchRelevantContent` is supported now
- `filterConfiguration`: Specifies the data source id of the Amazon Q application environment. The ISV will only have access to the data from the specified data source id. If there is no data source id specified, the ISV will have access to all the data sources.

```
# CreateDataAccessor actionConfigurations example
[
   {
        "action": "qbusiness:SearchRelevantContent",
        "filterConfiguration": {
        "documentAttributeFilter": {
          "equalsTo": {
            "name": "_data_source_id",
            "value": {
              "stringValue": "your_datasource_id"
            }
          }
        }
      }
   }
]
```

CLI example

The following CLI example shows how to create a data accessor and associate the necessary permissions with all end users enabled for this data accessor:

```
aws qbusiness create-data-accessor \
 --application-id ${qbusiness_application_id} \
```

```
 --principal ${isv_data_accessor_role_arn} \
 --action-configurations  ${action_configuration} \
 --display-name ${qbusiness_data_accessor_name} \
 --authentication-detail ${authentication_detail}

aws qbusiness associate-permission \
 --application-id ${qbusiness_application_id} \
 --statement-id ${statement_id} \
 --actions ${actions} \
 --principal ${isv_data_accessor_role_arn} \
 --conditions ${conditions}

aws sso-admin put-application-assignment-configuration \
 --application-arn ${qbusiness_data_accessor_idc_application_arn}\
 --no-assignment-required\
 --region ${idc_region}
```

The following CLI example shows how to add authentication details in your request:

```
# For tti based dataaccessor
"authenticationDetail": {
    "authenticationType": "AWS_IAM_IDC_TTI",
    "authenticationConfiguration": {
        "idcTrustedTokenIssuerConfiguration": {
            "idcTrustedTokenIssuerArn": "${IDC trusted token issuer created using ISV
 issuer URL}"
        }
    },
    "externalIds": [
        "${ISV tenantId}"
    ]
}

# For Authcode based dataaccessor
"authenticationDetail": {
    "authenticationType": "AWS_IAM_IDC_AUTH_CODE",
    "externalIds": [
        "${ISV tenantId}"
    ]
}
```

Completing the process to add a data accessor

After you grant a software provider (ISV) data accessor permissions, you'll need to provide AWS or the ISV with the following configuration parameters. They will reach out to you to source these configuration parameters. These values are required inputs when the ISV uses the `SearchRelevantContent` API operation to perform cross-account access of the data from your Amazon Q index.

Topics

- Using the AWS Management Console
- Using the AWS CLI;

These parameters are all easily accessed from the AWS Management Console:

1. Amazon Q Business application ID — This is the unique identifier of the Amazon Q Business application environment. It tells the ISV what Amazon Q application environment is associated with the Amazon Q index.
2. The Amazon Q Business application Region — This is the AWS Region where the Amazon Q Business application environment is created.
3. Amazon Q Business retriever ID — This is the unique identifier for the retriever. The retriever gets the data from the Amazon Q index configured by the Amazon Q customer.
4. Data accessor application ARN — This is the ISV Amazon Resource Name (ARN). It is used to identify the ISV when it is accessing a customer's Amazon Q index.
5. The Region for the Identity and Access Management (IAM) Identity Center (IDC) instance — This is the AWS Region where the IDC instance of the customer has been created.

The ISV can then begin retrieving content from the Amazon Q index by calling the `SearchRelevantContent` API. The `SearchRelevantContent` API follows Amazon Q Business access control standards by only retrieving data that the customer's end users have been given access to.

Using the AWS Management Console

To access these variables in the Amazon Q Business console:

1. Sign in to the AWS Management Console and choose the **Amazon Q Business** console.
2. Choose **Applications**, then select the name of your application environment from the list.
3. In the **Application details** page, you will see the **Application id** on this page and the application environment **Region** on the top right corner of the console top navigation bar.
4. From the left navigation, choose **Data sources**.
5. In the **Data sources** page, you will see the **Retriever id** on this page.
6. From the left navigation, choose **Data accessors**.
7. Choose the **Data accessor** from the **Data accessor(s) list** section.
8. In the **Data accessor details** page, you will see the **Data accessor IDC application ARN** on this page.
9. To get the IAM Identity Center (IDC) Region, you will need to open the IAM IDC console, Choose **Dashboard** and you can find the IDC **Region** in the Summary Settings section on that page.

Using the AWS CLI;

Amazon Q Business `applicationId` and the `dataAccessorArn` are included in the response of `GetDataAccessor` API. To get the IDC Region of your IDC instance and the IDC application environment, you need to visit IAM identity center page in the AWS Management Console.

```
# To get qbusiness application id
aws qbusiness list-applications
{
    "applications": [
        {
            "displayName": "your_qbusiness_application",
            "applicationId": ${qbusiness_application_id},
            "createdAt": ...,
            "updatedAt": ...,
            "status": "ACTIVE",
            "identityType": "AWS_IAM_IDC"
        }
    ]
}

# To get IDC application arn
aws qbusiness list-data-accessors --application-id ${qbusiness_application_id}
```

```
{
    "dataAccessors": [
        {
            "displayName": "Miro-3ajmo",
            "dataAccessorId": "7493bad6-df69-487c-b2b3-cd55bf01434c",
            "idcApplicationArn": "your_idc_application_arn",
            "principal": "arn:aws:iam::419356813857:role/
AwsQBusinessMiroRetrievalRole",
            ...
        }
    ]
}

# To get retriever id
aws qbusiness list-retrievers \
  --application-id ${qbusiness_application_id}
{
    "retrievers": [
        {
            "applicationId": ${qbusiness_application_id},
            "retrieverId": "your_retriever_id",
            "type": "NATIVE_INDEX",
            "status": "ACTIVE",
            "displayName": "..."
        }
    ]
}
```

Deleting or removing a data accessor's access from your Amazon Q index

You can remove a data accessor's permissions to your Amazon Q index using the Amazon Q Business console or the Amazon Q Business API using the AWS SDK, REST API, or AWS CLI. Once deleted, you will have to add the data and reconfigure access to grant the data accessor access again.

The following procedures show how you delete or remove a data accessor using the Amazon Q Business console or the AWS CLI.

Topics

- Using the Amazon Q Business console

- Using the AWS CLI;

Using the Amazon Q Business console

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. Choose **Applications**, then select the name of your application environment from the list.
3. From the left navigation, choose **Data accessors**.
4. From the **Data accessor** table, select the data accessor that you want to delete.
5. Choose **Actions**, then choose **Delete**.
6. Confirm your choice.

Using the AWS CLI;

```
aws qbusiness delete-data-accessor \
--application-id ${qbusiness_application_id} \
--data-accessors-id ${qbusiness_data_accessor_id}

aws qbusiness disassociate-permission \
--application-id ${qbusiness_application_id} \
--statement-id ${policy_statement_id}
```

Amazon Q embedded

Amazon Q embedded is a feature that lets you embed the Amazon Q Business assistant within websites that you trust. The Amazon Q assistant is powered by generative AI and can be configured to answer questions, provide summaries, generate content, and complete tasks based on your enterprise data. This allows your end users to receive immediate, permissions-aware responses from enterprise data sources, with citations.

For example, if you have a company intranet website, you can create an Amazon Q web experience by using your company data. You can then embed this web experience on your website. Your users can log in to the chat experience using their company credentials and ask the embedded Amazon Q Business chat experience questions. Your users receive responses based on the data sources used by the Amazon Q application environment.

Topics

- Prerequisites
- Add your website as an allowed URL
- Add Amazon Q embedded to your website
- Remove your website as an allowed URL

Prerequisites

Before you can embed the Amazon Q Business web experience in your websites, you must complete the following steps.

1. Get started with Amazon Q Business
2. Create an IAM Identity Center-integrated application, or Create an IAM federated application, or Create an anonymous access application and create your Amazon Q Business web experience.

Add your website as an allowed URL

To configure allowed websites for your existing web experience, you can use the Amazon Q Business console or the Amazon Q Business API.

> **Note**
>
> - The allowed *base URLs* must begin with `https://` or `http://`.
> - You must only submit a *base URL*, and not the full path. For example, `https://docs.aws.amazon.com`.

Using the console

1. Sign in to the Amazon Q console.
2. Choose **Applications**, then select the name of your application from the list.

> **Note**
>
> - Copy and save the **Deployed URL** for your Amazon Q application. You'll need this URL when you embed the web experience on your website.

- For anonymous applications, the **Deployed URL** must be generated every time using the `CreateAnonymousWebExperienceUrl` API operation. For more information, see Share an anonymous web experience.

3. From the left navigation pane, choose **Amazon Q embedded** under the **Enhancements** section.
4. On the main page, choose **Add allowed website** and enter the *base URL* of the website where you'll be embedding the Amazon Q Business web experience.

Using the AWS CLI

```
aws qbusiness update-web-experience \
  --application-id application-id \
  --web-experience-id web-experience-id \
  --origins origins

aws qbusiness get-web-experience \
  --application-id application-id \
  --web-experience-id experience-id
```

The `get-web-experience` operation will return the `defaultEndpoint`, which is the web experience URL that you will embed in your website.

Add Amazon Q embedded to your website

You can embed your Amazon Q Business web experience by adding an `<iframe>` element to your website with the **Deployed URL** or `defaultEndpoint` you copied earlier as the `src` value and a minimum width of *450 pixels* as follows.

```
<iframe src="Deployed-URL-or-defaultEndpoint" style="min-width: 450px;"/>
```

Once this <iframe> is added to the website, the Amazon Q Business chat assistant will show up and be ready to be used by your authenticated Amazon Q users.

Amazon Q Business users must provide user authentication credentials before they can use the embedded Amazon Q chat experience on your website. These credentials are the same as the credentials required for the Amazon Q web experience. To authenticate, Amazon Q opens a new

browser tab or window where users can enter their credentials. Once successfully authenticated, users can close this tab or window and begin using the embedded Amazon Q chat experience within the website.

Note

- For anonymous applications, the **Deployed URL** must be generated every time using the `CreateAnonymousWebExperienceUrl` API operation. For more information, see Share an anonymous web experience.
- If your browser has a limited cookie mode (ex. Incognito mode in Chrome), you may have to enable third-party cookies for Amazon Q embedded to work.
- The button for copying may not work without `allow="clipboard-read; clipboard-write"` attribute added to iframe

Remove your website as an allowed URL

To remove a website(s) from list of allowed websites, you can use the Amazon Q Business console or the Amazon Q Business API.

Using the console

1. Sign in to the Amazon Amazon Q Console.
2. Choose **Applications**, then select the name of your application from the list.
3. From the left navigation, choose **Amazon Q embedded** under the **Enhancements** section.
4. On the main page, select the website that you want to remove and choose **Remove** and confirm your choice.

Using the AWS CLI

To remove the website from the list of allowed websites, you will need to use the `get-web-experience` operation to get a list of all your allowed website URLs `origins` and remove the website that you no longer want to work with Amazon Q embedded and resubmit the rest of the URLs using the `update-web-experience` operation. Otherwise, all your other allowed websites will also be removed.

```
 aws qbusiness get-web-experience \
  --application-id application-id \
  --web-experience-id web-experience-id \

aws qbusiness update-web-experience \
  --application-id application-id \
  --web-experience-id web-experience-id \
  --origins origins
```

Note

You will need to remove the `<iframe>` element from that website as it will no longer work.

Integrations

Amazon Q Business integrations enhance user productivity by bringing AI-powered assistance directly into daily workflows. To get started, choose the integrations you want Amazon Q to integrate with. Then, deploy your integrations to bring Amazon Q's capabilities directly within those enterprise tools.

In this section, you will find the different integrations that Amazon Q Business supports and how to configure them for your company.

The following is a list of the integrations supported by Amazon Q Business.

- **Browser extensions** (Google Chrome, Microsoft Edge, and Mozilla Firefox)

  Available for: Lite and Pro tiers
- **Slack**

  Available for: Pro tier only
- **Microsoft Teams**

  Available for: Pro tier only
- **Microsoft Outlook**

  Available for: Pro tier only
- **Microsoft Word**

Available for: Pro tier only

Topics

- Enhancing web browsing with Amazon Q Business
- Integrating Slack with Amazon Q Business
- Integrating Microsoft Teams (Teams) with Amazon Q Business
- Integrating Microsoft Outlook with the Amazon Q Business Add-in
- Integrating Microsoft Word with the Amazon Q Business Add-in
- IAM roles and trust policy for your integrations

Enhancing web browsing with Amazon Q Business

The Amazon Q Business browser extension enhances your users' web browsing experience. As your users browse the web, the Amazon Q Assistant can answer questions, provide summaries, generate content, and complete tasks based on data made available to it or from its general knowledge right in their browser enhancing your users' productivity by bringing Amazon Q's AI-powered assistance directly into their daily workflows.

With the Amazon Q browser extension your users can:

- Summarize a snapshot of any web page
- Ask questions about one or more web pages
- Access Amazon Q's general knowledge and your company's knowledge
- Upload documents and use other features available in the Amazon Q web experience.

Topics

- Configuring the Amazon Q Business browser extension for use
- Removing the browser extension as an integration
- Using the Amazon Q Business browser extension

Configuring the Amazon Q Business browser extension for use

After installation and authentication, your users can access Amazon Q while browsing the web.

Note

- Amazon Q does not support users who authenticate using external SAML providers.
- The Safari browser is not supported.
- Amazon Q Business does not use user data for service improvement or for training its underlying large language models (LLMs). For more information, see Amazon Q Business Service improvement.
- Upload your documents and have Amazon Q answer contextual questions about them.

Topics

- Prerequisites for integrating the Amazon Q browser extension
- Integrating the browser extension with Amazon Q Business
- Activating and deploying the browser extension

Prerequisites for integrating the Amazon Q browser extension

As admins, before you can integrate the Amazon Q Business browser extension, you must complete the following steps.

1. Get started with Amazon Q Business
2. Create an IAM Identity Center-integrated application or Create an IAM federated application environment and create your Amazon Q Business web experience.
3. To use this feature, do the following
   - Enable **Allow end users to send queries directly to the LLM** in your Admin controls and guardrails. For more information, see the Response settings topic in Admin controls and guardrails and `chatMode` if you are configuring programmatically.
   - If you are using the IAM Identity Center or OpenID Connect (OIDC) provider in IAM, make sure your IAM role for an Amazon Q Business web experience using IAM Federation is up to date. For more information, see IAM role for an Amazon Q Business web experience using IAM Federation.

Integrating the browser extension with Amazon Q Business

To use the Amazon Q Business browser extension, you must allow it to connect to your Amazon Q Business application environment and web experience. To do this, admins can use the Amazon Q console, API, SDK, or AWS CLI.

Topics

- Using the console
- Using the AWS API

Using the console

1. Sign in to the Amazon Q console.
2. Choose **Applications**, then select the name of your application environment from the list.
3. Choose **Integrations** under **Enhancements**.
4. Choose **Edit** in the **Browser extensions** section on the main page.
5. Choose the **Browser extensions** your want integrate with.

Using the AWS API

Admin users can enable your browser extensions using the `UpdateWebExperience` and `CreateWebExperience` operations.

Activating and deploying the browser extension

After enabling the browser extension, complete these steps to activate and deploy it:

1. Allow-list URLs. If you are using
   a. An OIDC provider like Okta: you must configure your identity provider (IdP) to support browser extension as follows. You will need to consult your provider on how to do this.
      i. Make sure you enable refresh grants
      ii. Allow-list the following URLs with the IdP
         A. Mozilla based browsers — `https://ba6e8e6e4fa44c1057cf5f26fba9b2e788dfc34f.extensions.allizom.org`
         B. Chromium based browsers — `https://feihpdljijcgnokhfoibicengfiellbp.chromiumapp.org`

   b. IAM Identity Center, the above is not required and you can move to the next step of installing the browser extension for your users.

2. Install the browser extension for all users using the software deployment processes of your organization. The following is some information about policy settings from the browser vendors using mobile device management (MDM) software that may be helpful:
   a. Firefox policy settings: https://mozilla.github.io/policy-templates/#extensionsettings
   b. Chrome policy settings: https://chromeenterprise.google/policies/#ExtensionSettings
   c. Edge policy settings: https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#extensionsettings and guide: https://learn.microsoft.com/en-us/deployedge/microsoft-edge-manage-extensions-ref-guide
3. Provide your selected users the browser store URL + Web experience URL so they can download and install the browser extension and connect to Amazon Q.

Removing the browser extension as an integration

To disable the browser extension to your existing web experience, Admin users can use the Amazon Q Business console or the Amazon Q Business API, AWS SDK, or AWS CLI.

Topics

- Using the console
- Using the AWS API
- Blocking and removing the browser extension

Using the console

1. Sign in to the Amazon Q console.
2. Choose **Applications**, then select the name of your application environment from the list.
3. Choose **Integrations** under **Enhancements**.
4. Choose **Edit** in the **Browser extensions** section on the main page.
5. Deselect the **Browser extensions** you no longer want integrate with.

Using the AWS API

You can disable browser extensions using the `UpdateWebExperience` API

Blocking and removing the browser extension

Once you disable your browser extension, your users will no longer be able to login. However, you will still need to take steps to uninstall the extension on user's browser via

- Uninstall the browser extension for all users by updating the policy settings using the mobile device management software (MDM) using one of the following:
  - Firefox policy settings: https://mozilla.github.io/policy-templates/#extensionsettings
  - Chrome policy settings: https://chromeenterprise.google/policies/#ExtensionSettings
  - Edge policy settings: https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#extensionsettings and guide: https://learn.microsoft.com/en-us/deployedge/microsoft-edge-manage-extensions-ref-guide

Using the Amazon Q Business browser extension

The browser extension is available to Amazon Q Business users on Google Chrome, Mozilla Firefox, and Microsoft Edge browsers.

Topics

- Prerequisites for using the browser extension
- Install and configure the browser extension
- Common use cases for using the Amazon Q Business browser extension
- Considerations for using the Amazon Q Business browser extension
- Troubleshooting the Amazon Q Business browser extension

Prerequisites for using the browser extension

- You must be a user
- Your Amazon Q Admin must connect the browser extension with your Amazon Q Business web experience.
- Supported browsers are Google Chrome, Mozilla Firefox, Microsoft Edge, but reach out to their admin to find out which browsers are enabled for use with Amazon Q.

Install and configure the browser extension

- To set up your browser extension, either wait for your IT department to configure and install it automatically, or follow their installation instructions.

  The following are browser extensions from third-party providers that may be helpful.

  - Mozilla based browsers — https://addons.mozilla.org/en-GB/firefox/addon/amazon-q-business/
  - Chromium based browsers (including Microsoft Edge) — https://chromewebstore.google.com/detail/amazon-q-business/feihpdljijcgnokhfoibicengfiellbp
- If you have an Amazon Q Business web experience and would like to connect to it, navigate to it in one of your other browser windows, the extension will automatically detect and suggest the link to connect your Amazon Q web experience. If not, you will need to paste the link to your Amazon Q web experience at the time of authenticating to the Amazon Q browser extension. Your browser extension will remember this link for future logins, but you can always choose a different Amazon Q web experience link.
- Once you have successfully logged on, you can use your Amazon Q browser extension.

> **Tip**
>
> You can also *pin* your Amazon Q browser extension to have it readily accessible while using your browser. Instructions for this are specific to your browser of choice. The following third-party information about pinning extensions might be helpful.
>
> - Google Chrome — https://www.howtogeek.com/683099/how-to-pin-and-unpin-extensions-from-the-chrome-toolbar
> - Mozilla Firefox — https://support.mozilla.org/en-US/kb/extensions-button#w_manage-pinned-extensions
> - Microsoft Edge — https://www.microsoft.com/en-us/edge/features/pin-to-taskbar

Safari browsers are not supported at the time.

Common use cases for using the Amazon Q Business browser extension

The following are some of the common use cases that will help you make the best use of your Amazon Q Business browser extension:

1. **Summarize a page**
   a. Open the Amazon Q Business browser extension
   b. Login and navigate to the web page that you want to summarize.
   c. Use the **summarize** for a summary of a snapshot of that web page for the moment when you navigated to it.
   d. Now your conversation contains a snapshot of this web page. You can continue to chat about the web page and ask followup questions.
2. **Add web pages and files as context to an Amazon Q conversation**
   a. Switch to General Knowledge mode.
   b. If you have clicked on the summarize button, the current web page is already in your conversation context. To add the current web page to the conversation without summarizing the page:
      i. Choose the paperclip icon
      ii. Select add current page
   c. Ask questions about the current web page snapshot.
   d. To add a file, choose the paper clip icon and browse to the file of your choice (~50MB maximum size limit, ~3.75MB per image)
   e. You can have up to a total of 20 web page snapshots or files in your conversation. To add another web page, navigate to the next web page that you'd like to add and repeat the first step.
   f. To remove an attachment, choose the paper clip icon and remove the web page snapshots or files of your choice.
3. **Access Amazon Q Business' Knowledge from your company data sources**
   a. Switch to Company Knowledge mode
   b. Ask Q Business questions about your company's data sources
   c. Get source attribution for your data sources
4. **Reset the context of your current conversation**
   a. To reset the context of your current conversation, choose the new chat bubble icon. Your chat will be free of past attachments and web page snapshots.

> **Important**
>
> The Amazon Q Business browser extension integration does not support actions or plugins.

Considerations for using the Amazon Q Business browser extension

1. Amazon Q Business does not use customer data for service improvement or for improving its underlying large language models (LLMs). Also, none of the data you include in your browser extension conversations will be indexed into your company's Amazon Q Business instance. For more information, see Amazon Q Business Service improvement.
2. You can access all history of previous conversations (including attachments to those conversations) that have not been deleted from the Amazon Q web experience conversation history.
3. All conversations with Amazon Q including uploaded web page snapshots and files from the browser extension will be deleted after 30 days of inactivity.
4. If you close the Amazon Q browser extension, it will start a new conversation the next time you reopen it.
5. Amazon Q's responses aren't always 100% accurate. For more information, see Hallucination in the topic Key concepts of Amazon Q Business.

Troubleshooting the Amazon Q Business browser extension

- **My admin has enabled the browser extension, but I'm unable to login.**

  Try having a conversation on your Amazon Q web experience first and then try the browser extension again. If this doesn't work, then contact your Amazon Q admin or IT department.

- **I am getting a "Can't access document" error.**

  This happens when a web uses an unsupported format from which the browser extension is unable to pull relevant data to provide a helpful response. If you encounter this error and would like your web page to be supported, please submit feedback via the feedback button in the browser extension

- **Amazon Q doesn't respond helpfully or doesn't use the context of the web page I added.**

Try starting a new chat and adding the web page snapshot or file again. If it still does not work, submit feedback using the feedback button and include any non-confidential details about the type of web page where the extension failed,

- **I get the error, 'To use this browser extension, your administrator needs to enable "Allow end users to send queries directly to the LLM" in the Amazon Q Business console'**.

  Contact your Admin or IT department with the error.
- **Amazon Q doesn't recognize updated information when my web page changes.**

  Amazon Q only has access to a snapshot of a web page. Similar to a photograph, this is all the information in the web page from the time it was uploaded to Amazon Q. To refresh the snapshot of your page, remove the current snapshot of the web page, choose a refreshed snapshot of the page, and choose **Summarize** or **Upload** for summarizing or further contextual analysis.

Integrating Slack with Amazon Q Business

Amazon Q Business can enhance your users' Slack experience by increasing their productivity, bringing Amazon Q's AI-powered assistance directly into their daily workflows. With the Amazon Q assistant in Slack, users can access Amazon Q's knowledge without context switching during communications. Users can ask Amazon Q questions about its company knowledge, general knowledge (if enabled), and uploaded files using the Slack AI assistant side panel. Users can also mention *@Amazon Q Business* in Slack threads to add it as a collaborator and ask contextual questions about the thread such as "*what are the action items from this thread?*" or "*summarize this thread*".

With the Amazon Q Slack integration your users can do the following:

- Mention *@Amazon Q Business* in conversations to add it as a collaborator.
- Ask contextual questions about conversations like "summarize this thread".
- Access Amazon Q's general knowledge.
- Access their company's knowledge (if enabled).
- Upload documents and other features that they have access to in the using the Amazon Q web experience.

Topics

- Configuring the Amazon Q Business Slack integration for use
- Using the Amazon Q Business Slack App

Configuring the Amazon Q Business Slack integration for use

The Amazon Q Business integration for Slack is only available for use by Amazon Q Business Pro users.

Note

- When Amazon Q is invoked by a user in a public Slack channel, it generates responses based on the invoking user's permissions, which may include content that other channel members aren't authorized to access. To prevent unintended exposure of sensitive information, carefully evaluate the use of Amazon Q in public channels.
- The Amazon Q Business customer integrating Slack must have a paid Slack workspace.
- Amazon Q only supports user access management through IAM Identity Center for Slack integrations. This includes authentication using external SAML providers through IAM Identity Center. To integrate Slack with Amazon Q, you must create an IAM Identity Center-integrated application. For more information, see Create an IAM Identity Center-integrated application.
- Amazon Q doesn't support Slack integrations for Amazon Q applications using IAM federation for user access management.
- Access using the Amazon Q Business API is not supported at this time.
- Amazon Q Business does not use your user data for service improvement or for training its underlying large language models (LLMs). For more information, see Amazon Q Business Service improvement.
- Uploading documents and conversations will follow the same behavior as the web experience. For more information, see the Chat and file uploads section in the Using web experience topic.

Topics

- Prerequisites
- Adding an Amazon Q Business integration for Slack
- Removing Slack as an integration

Prerequisites

As admins, before you can add the Amazon Q Business integration to your Slack, you must complete the following steps:

1. Must have a paid Slack workspace
2. Get started with Amazon Q Business
3. Create an IAM Identity Center-integrated application environment environment and create your Amazon Q Business web experience.

   > **Note**
   >
   > Amazon Q doesn't support Slack integrations for Amazon Q applications using IAM federation for user access management.

4. Optionally, to enhance your end users' experience with Amazon Q in Slack, you can enable **Allow end users to send queries directly to the LLM** in your Admin controls and guardrails. For more information, see the Response settings topic in Admin controls and guardrails and `chatMode` if you are configuring programmatically.
5. Add the two IAM roles and trust policies for adding integrations. For more information, see IAM roles and trust policy for your integrations
6. Admin access to your Slack workspace.
7. Your Slack workspace ID. Your WorkSpace ID must start with a *T*. One way to find your Slack workspace ID is by navigating to your Slack workspace and starting a chat with the *Slack Developer Tools* app running the `/sdt whoami` command. For more information, see Locate your Slack URL or ID in the Slack help center.

Adding an Amazon Q Business integration for Slack

To use the Amazon Q Business Slack integration, you must allow it to connect to your Amazon Q Business application environment and web experience. To do this, admins can use the Amazon Q Business console, API, SDK, or AWS CLI.

> **Note**
>
> This integration can only be added using the AWS Management Console at this time.

Topics

- Using the console
- Installing the Amazon Q Business App in your Slack workspace

Using the console

1. Sign in to the Amazon Q console.
2. Choose **Applications**, then select the name of your application environment from the list.
3. Choose **Integrations** under **Enhancements**.
4. Choose **Add integration** from the **Integrations** section on the main page.
5. Choose **Slack** as your integration.
6. On the **Add Slack integration page**, enter the **Name** of your integration. This is the display name for the integration resource in AWS.
7. Add a **description** (optional).
8. Enter your Slack workspace ID. This is a unique identifier of your Slack workspace starting and can be found using the Slack developer tools app. To find your workspace ID:
    a. Navigate to your Slack workspace and in “Apps” search for “Slack Developer Tools”.
    b. Open the Slack Developer Tools app and run the command /sdt whoami
    c. You will receive a response that contains your Workspace ID starting with a “T”
    d. For other ways to locate your workspace ID, refer to Locate your Slack URL or ID in the Slack help center.
9. Choose the type of **Service access** method that you want the Slack integration to use as authorization while accessing your service. You can **Create a new service role** or **Use an existing service role**. For more information, see IAM role for allowing the integration to call Amazon Q Business on your end user's behalf.
10. Choose the **Access management access** for the Slack integration to authorize to connect to IAM Identity center. For more information, see IAM role for allowing Amazon Q Business to monitor the resources that the integration creates in your account.
11. Optionally, add any **Tags** that are relevant for this Slack integration.
12. Choose **Add integration**.
13. Once the integration has been successfully created, you will move to the **Integration details page**.

14. Choose **Deploy integration**.
15. Choose **Access Slack**.

> **Note**
>
> This link will take you to the Slack domain outside of AWS.

16. You will continue this procedure within the Slack domain.

Installing the Amazon Q Business App in your Slack workspace

The following instructions show how to install the Amazon Q Business App in your Slack workspace using a link from the Amazon Q console as shown in the previous topic.

> **Note**
>
> - Only a Slack workspace owner can use the link to install the Amazon Q App into your Slack workspace.
> - There can be only one instance of the Amazon Q App per Slack workspace. That instance will be connected to the application environment that integration was configured with in the previous topic.
> - You may see a "This app is not approved by Slack banner." This message can be ignored.

1. The link will open to a Slack login page where after you login (as admin) you will need to find and be asked to install the Amazon Q app within your Slack workspace.
2. Choose **Allow** to install your Amazon Q App for Slack.
3. Once the installation is complete, you will see the page confirming that the **Congratulations! Your Slack App has been successfully installed.**
4. Choose **Open the Amazon Q Business App in Slack**.
5. This will open your Slack workspace where all users will be required to sign-in.

Removing Slack as an integration

To remove the Slack integration, admin users can use the Amazon Q Business console.

> **Note**
>
> This integration can only be removed using the AWS Management Console at this time.

Using the console

1. Sign in to the Amazon Q console.
2. Choose **Applications**, then select the name of your application environment from the list.
3. Choose **Integrations** under **Enhancements**.
4. Find and select your Slack integration from the **Integrations** section on the main page.
5. Choose **Delete** and confirm your choice.

Once you disable your Slacks integration, your users will no longer be able to login. However you will still need to take steps to uninstall the Amazon Q Business App in your Slack Workspace.

Using the Amazon Q Business Slack App

The Amazon Q Business Slack app is available to all Amazon Q Business users.

Topics

- Prerequisites
- Install and configure the Amazon Q Business App in Slack
- Features of the Amazon Q Business Slack App
- Considerations for using the Amazon Q Business App for Slack
- Troubleshooting the Amazon Q Business App for Slack

Prerequisites

- Your Amazon Q admin must connect the Amazon Q Business Slack app to your Slack workspace.

Install and configure the Amazon Q Business App in Slack

The following are instructions on how to install the Amazon Q Business App in Slack:

1. Open and login to the Slack workspace for your company.

2. Choose **More** in the left navigation, then select **Automations**.
3. Choose **Apps**.
4. Choose **+ Add apps**
5. Search for "Amazon Q Business" and choose **Amazon Q Business**
6. This will take you to the **About** page. Choose the 3 vertical dots (that say "more actions") to the right of the New Chat button.
7. Choose **add assistant to top bar**
8. You will now see a **Q** icon/logo on the top bar on the right where you can **access and chat with Amazon Q Business**

For more information, see Understand AI apps in Slack in the Slack help center.

Features of the Amazon Q Business Slack App

Following are some of the features supported by the Amazon Q Slack App:

- In direct messages (DMs) to the Amazon Q Business contact, it responds to all messages and queries.
- In channels it responds only to @mentions, and always replies in thread.
- Thumbs up and down buttons to track feedback and help improve performance over time.
- Provides Source Attribution - see references to sources used by Amazon Q Business.
- It tracks the conversation and applies context.
- Process up to 5 attached files for contextual question answering, summaries, etc.

> ⚠ **Important**
>
> The Amazon Q Business Slack integration does not support actions or plugins.

Considerations for using the Amazon Q Business App for Slack

1. When Amazon Q is invoked by a user in a public Slack channel, it generates responses based on the invoking user's permissions, which may include content that other channel members aren't authorized to access. To prevent unintended exposure of sensitive information, carefully evaluate the use of Amazon Q in public channels.

2. Amazon Q Business does not use customer data for service improvement or for improving its underlying large language models (LLMs). Also, none of the data you include in your browser extension conversations will be indexed into your company's Amazon Q Business instance. For more information, see Amazon Q Business Service improvement.
3. The Amazon Q Business Slack app will have access to the same knowledge available in the corresponding Amazon Q Business web experience.
4. To reset, start new conversation, direct message as a *New chat*.
5. When you upload a file, the Amazon Q Slack app will only be able to respond from the file (and general knowledge if your Amazon Q admin has enabled it). Start a new chat if you want to return to getting answers from company knowledge.
6. Closing the Amazon Q Business Slack app side panel will end the current conversation. Users can review past conversations in Slack or all conversations from all channels (Slack, browser extensions, etc.) in your Amazon Q Business web experience. You can access all the history of previous conversations including, the names of the attachments in those conversations.
7. All conversations in Amazon Q Business are deleted after 30 days of inactivity. Slack may store conversations for longer depending on your company's Slack conversation history rules.
8. Amazon Q may provide inaccurate responses at times. For more information, see Hallucination in the topic Key concepts of Amazon Q Business.

Troubleshooting the Amazon Q Business App for Slack

My admin has enabled the Amazon Q Business app for Slack, but I'm unable to login.

> Try having a conversation on your Amazon Q web experience first and then try Slack again. If this doesn't work, then contact your Amazon Q admin or IT department.

I am getting a "Can't access document" error.

> This happens when a document uses an unsupported format from which Amazon Q app is unable to pull relevant data to provide a helpful response. If you encounter this error and would like your file format to be supported, please submit feedback via the feedback button in the browser extension.

Amazon Q doesn't respond helpfully or doesn't use the context of the document I added.

> Try starting a new chat and adding the document again. If it still does not work, contact your Amazon Q Business admin for further support.

Integrating Microsoft Teams (Teams) with Amazon Q Business

Amazon Q Business can enhance your users' Microsoft Teams (Teams) experience by increasing their productivity, bringing Amazon Q's AI-powered assistance directly into their daily workflows. With the Amazon Q Assistant in Teams, users can access Amazon Q's knowledge without context switching during communications. Users can ask Amazon Q questions about its company knowledge, general knowledge (if enabled), and uploaded files using the Teams AI assistant side panel. Users can also mention *@Amazon Q Business* in Teams threads to add it as a collaborator and ask contextual questions about the thread such as "*what are the action items from this thread?*" or "*summarize this thread*".

With the Amazon Q Microsoft Teams (Teams) integration your users can do the following:

- Mention *@Amazon Q Business* in conversations to add it as a collaborator.
- Access Amazon Q's general knowledge.
- Access their company's knowledge (if enabled).
- Upload documents and other features that they have access to in the using the Amazon Q web experience.

Topics

- Configuring the Amazon Q Business Microsoft Teams (Teams) integration for use
- Using the Amazon Q Business Microsoft Teams app

Configuring the Amazon Q Business Microsoft Teams (Teams) integration for use

Note

- When Amazon Q is invoked by a user in a public Teams channel, it generates responses based on the invoking user's permissions, which may include content that other channel members aren't authorized to access. To prevent unintended exposure of sensitive information, carefully evaluate the use of Amazon Q in public channels.
- The Amazon Q Business customer integrating Microsoft Teams (Teams) must have a paid Teams organization.

- Amazon Q supports users who authenticate using external SAML providers through IAM Identity Center. For more information, see Create an IAM Identity Center-integrated application.
- Amazon Q application environment created with IAM Federation do not support integrations with Teams at this time.
- Access using the Amazon Q Business API is not supported at this time.
- Amazon Q Business does not use your user data for service improvement or for training its underlying large language models (LLMs). For more information, see Amazon Q Business Service improvement.
- Uploading documents and conversations will follow the same behavior as the web experience. For more information, see the Chat and file uploads section in the Using web experience topic.

Topics

- Prerequisites
- Adding an Amazon Q Business integration for Microsoft Teams
- Removing Microsoft Teams as an integration

Prerequisites

As admins, before you can add the Amazon Q Business integration to your Microsoft Teams (Teams), you must complete the following steps:

1. You must have a Microsoft 365 Business subscription and be a *Global Admin* or someone with administrative permissions, specifically `AppCatalog.ReadWrite.All`.
2. Get started with Amazon Q Business
3. Create an IAM Identity Center-integrated application environment environment and create your Amazon Q Business web experience.

> **Note**
>
> IAM federated application environment environments do not support integrations with Teams.

4. Optionally, to enhance your end users' experience with Amazon Q in Teams, you can enable *Allow end users to send queries directly to the LLM* in your Admin controls and guardrails. For more information, see the Response settings topic in Admin controls and guardrails and `chatMode` if you are configuring programmatically.
5. Add the two IAM roles and trust policies for adding integrations. For more information, see IAM roles and trust policy for your integrations
6. Your Microsoft 365 tenant ID. For more information, see How to find your tenant ID - Microsoft Entra in the Microsoft Learn portal.

Adding an Amazon Q Business integration for Microsoft Teams

To use the Amazon Q Business Teams integration, you must allow it to connect to your Amazon Q Business application environment and web experience. To do this, admins can use the Amazon Q Business console, API, SDK, or AWS CLI.

> **Note**
>
> This integration can only be added using the AWS Management Console at this time.

Topics

- Using the console
- Installing the Amazon Q Business app in your Microsoft Teams organization

Using the console

1. Sign in to the Amazon Q console.
2. Choose **Applications**, then select the name of your application environment from the list.
3. Choose **Integrations** under **Enhancements**.
4. Choose **Add integration** from the **Integrations** section on the main page.
5. Choose **Microsoft Teams** as your integration.
6. On the **Add Teams integration page**, enter the **Name** of your integration. This is the display name for the integration resource in AWS.
7. Add a **description** (optional).

8. Enter your **Teams Tenant ID**. This can be found in the *Microsoft Entra Admin Center*. For more information, see How to find your tenant ID - Microsoft Entra
9. Choose the type of **Service access** method that you want the Teams integration to use as authorization while accessing your service. You can **Create a new service role** or **Use an existing service role**. For more information, see IAM role for allowing the integration to call Amazon Q Business on your end user's behalf.
10. Choose the **Access management access** for the Teams integration to authorize to connect to IAM Identity center. For more information, see IAM role for allowing Amazon Q Business to monitor the resources that the integration creates in your account.
11. Optionally, add any **Tags** that are relevant for this Teams integration.
12. Choose **Add integration**.
13. Once the integration has been successfully created, you will move to the **Integration details page**.
14. Choose **Deploy integration**.
15. Choose **Access Teams**.

> **Note**
>
> This link will take you to the Teams domain outside of AWS.

16. You will continue this procedure within the Teams domain.

Installing the Amazon Q Business app in your Microsoft Teams organization

The following instructions show how to install the Amazon Q Business App in your Microsoft Teams (Teams) workspace using a link from the Amazon Q console as shown in the previous topic.

> **Note**
>
> - Only a Teams *Global Admin* or someone with administrative permissions can add the Amazon Q Business App to your Teams organization, specifically `AppCatalog.ReadWrite.All`.
> - There can be only one instance of the Amazon Q App per Teams organization. That instance will be connected to the application environment that the Teams integration was configured with in the previous topic.

1. Open the link and login as Global Admin or or someone with administrative permissions can add the Amazon Q Business App to the Microsoft Teams admin center for your organization.
2. Choose **Teams apps** in the left navigation.
3. Choose **Amazon Q Business** from the list of available apps.
4. Review and grant admin consent by choosing the **Permissions** tab and reviewing the permissions and choose **Grant admin consent**.

   > **Note**
   >
   > If permissions are already granted, proceed to the end of the procedure, there is no further action required.

5. Authenticate and choose **Accept** for Amazon Q Business app.
6. Confirm that an app titled **Amazon Q Business Permissions** tab now says **Admin consent granted for all required permissions**.

All users assigned to the app from the **Teams admin center** can now find the app in the **Built for your org** section of the **Apps** page of their Teams app.

Removing Microsoft Teams as an integration

To remove the Microsoft Teams (Teams) integration, admin users can use the Amazon Q Business console.

> **Note**
>
> This integration can only be removed using the AWS Management Console at this time.

Using the console

1. Sign in to the Amazon Q console.
2. Choose **Applications**, then select the name of your application environment from the list.
3. Choose **Integrations** under **Enhancements**.
4. Find and select your Teams integration from the **Integrations** section on the main page.
5. Choose **Delete** and confirm your choice.

Once you disable your Microsoft Teams (Teams) integration, your users will no longer be able to login. However you will still need to take steps to uninstall the Amazon Q Business App in your Teams organization.

Using the Amazon Q Business Microsoft Teams app

Topics

- Prerequisites
- Install and configure the Amazon Q Business app in Microsoft Teams
- Features of the Amazon Q Business Microsoft Teams bot
- Considerations using the Amazon Q Business bot for Microsoft Teams (Teams)
- Troubleshooting the Amazon Q Business app for Microsoft Teams

Prerequisites

- You must have an Amazon Q Business user subscription.
- You must have a Microsoft 365 Business subscription.
- Your Amazon Q admin must connect the Amazon Q Business App to your Microsoft Teams organization.

Install and configure the Amazon Q Business app in Microsoft Teams

The following are instructions on how to install the Amazon Q app in Microsoft Teams (Teams):

1. Open and login to the Teams organization for your company.
2. Go to **Apps** on the left navigation and search for *Amazon Q Business*
3. Choose **Amazon Q Business**
4. You will now see a **Q** icon/logo on the top bar on the right where you can access and chat with Amazon Q Business.

For more information, see Chat with a bot in Microsoft Teams from Microsoft support.

Features of the Amazon Q Business Microsoft Teams bot

Following are some of the features supported by the Amazon Q Microsoft Teams (Teams) App:

- In direct messages (DMs) to the Amazon Q contact, it responds to all messages and queries.

- In channels it responds only to @mentions, and always in replies.
- Thumbs up and down buttons to track feedback and help improve performance over time.
- Provides Source Attribution - see references to sources used by Amazon Q Business.
- It tracks the conversation and applies context.
- Process up to 5 attached files for contextual question answering, summaries, etc. JPEG/JPG image file types are not supported as file uploads in the Teams integration.

> **Important**
>
> The Amazon Q Business Microsoft Teams integration does not support actions or plugins.

Considerations using the Amazon Q Business bot for Microsoft Teams (Teams)

1. When Amazon Q is invoked by a user in a public Teams channel, it generates responses based on the invoking user's permissions, which may include content that other channel members aren't authorized to access. To prevent unintended exposure of sensitive information, carefully evaluate the use of Amazon Q in public channels.
2. Amazon Q Business does not use customer data for service improvement or for improving its underlying large language models (LLMs). Also, none of the data you include in your Teams conversations will be indexed into your company's Amazon Q Business instance. For more information, see Amazon Q Business Service improvement.
3. The Amazon Q Business Teams app will have access to the same knowledge available in the corresponding Amazon Q Business web experience.
4. To reset, start new conversation, using the */new_conversation* command.
5. When you upload a file, the Amazon Q bot for Teams will only be able to respond from the file (and general knowledge if your Amazon Q admin has enabled it). Start a new chat if you want to return to getting answers from company knowledge.
6. Closing the Amazon Q Business bot for Teams side panel will end the current conversation. Users can review past conversations in Teams or all conversations from all channels (Teams, browser extensions, etc.) in your Amazon Q Business web experience. You can access all the history of previous conversations including, the names of the attachments in those conversations.
7. All conversations in Amazon Q Business are deleted after 30 days of inactivity. Teams may store conversations for longer depending on your company's Teams conversation history rules.

8. Amazon Q may provide inaccurate responses at times. For more information, see Hallucination in the topic Key concepts of Amazon Q Business.

Troubleshooting the Amazon Q Business app for Microsoft Teams

My admin has enabled the Amazon Q Business app for Microsoft Teams (Teams), but I'm unable to login.

Try having a conversation on your Amazon Q web experience first and then try Teams again. If this doesn't work, then contact your Amazon Q admin or IT department.

I am getting a "Can't access document" error.

This happens when a document uses an unsupported format from which Amazon Q app is unable to pull relevant data to provide a helpful response. If you encounter this error and would like your file format to be supported, please submit feedback via the feedback button.

Amazon Q doesn't respond helpfully or doesn't use the context of the document I added.

Try starting a new chat and adding the document again. If it still does not work, contact your Amazon Q Business admin for further support.

Integrating Microsoft Outlook with the Amazon Q Business Add-in

Amazon Q Business can enhance your users' Microsoft Outlook (Outlook) experience by increasing their email productivity, bringing Amazon Q's AI-powered assistance directly into their daily email workflows. As your users use their email, the Amazon Q Add-in can answer questions, provide summaries, draft responses and get insights from emails threads it has access to or from its general knowledge right in your Outlook enhancing your users' email productivity by bringing Amazon Q's AI-powered assistance directly into their daily email workflows.

With the Amazon Q Outlook Add-in your users can:

- Summarize your emails
- Draft contextual responses
- Access Amazon Q's company knowledge and general knowledge
- Upload documents and use other features available in the Amazon Q web experience.

Topics

- Configuring the Amazon Q Business Microsoft Outlook Add-in for use
- Removing the Amazon Q Business Add-in as a Microsoft Outlook integration
- Using the Amazon Q Business Add-in for Microsoft Outlook

Configuring the Amazon Q Business Microsoft Outlook Add-in for use

Note

- The Amazon Q Business customer integrating Microsoft Outlook (Outlook) must have a paid Outlook organization.
- Amazon Q supports users who authenticate using external SAML providers through IAM Identity Center. For more information, see Create an IAM Identity Center-integrated application.
- Amazon Q application environment created with IAM federation does not support the Outlook Add-in.
- Access using the Amazon Q Business API is not supported at this time.
- Amazon Q Business does not use user data for service improvement or for training its underlying large language models (LLMs). For more information, see Amazon Q Business Service improvement.
- Uploading documents and conversations will follow the same behavior as the web experience. For more information, see the Chat and file uploads section in the Using web experience topic.

Topics

- Prerequisites for integrating the Amazon Q Microsoft Outlook Add-in
- Integrating Microsoft Outlook with the Amazon Q Business Add-in

Prerequisites for integrating the Amazon Q Microsoft Outlook Add-in

As admins, before you can integrate the Amazon Q Business Microsoft Outlook (Outlook) Add-in, you must complete the following steps.

1. You must have a Microsoft 365 Business subscription and be a *Global Admin* or someone with administrative permissions, specifically `AppCatalog.ReadWrite.All`.

2. You need your Microsoft 365 tenant ID. For more information, see How to find your tenant ID - Microsoft Entra in the *Microsoft Learn portal*.
3. Get started with Amazon Q Business
4. Create an IAM Identity Center-integrated application and create your Amazon Q Business web experience.

> **Note**
>
> IAM federated application environments do not support integrations with Outlook.

5. Add the two IAM roles and trust policies for adding integrations. For more information, see IAM roles and trust policy for your integrations.
6. To use this feature, you must enable **Allow end users to send queries directly to the LLM** in your Admin controls and guardrails. For more information, see the Response settings topic in Admin controls and guardrails and `chatMode` if you are configuring programmatically.

Integrating Microsoft Outlook with the Amazon Q Business Add-in

To use the Amazon Q Business Add-in for Microsoft Outlook, you must allow it to connect to your Amazon Q Business application environment and web experience.

> **Note**
>
> This integration can only be added using the Amazon Q Business console.

Using the console

1. Sign in to the Amazon Q Business console.
2. Choose **Applications**, then select the name of your application environment from the list.
3. Choose **Integrations** under **Enhancements**.
4. Choose **Add integration** from the **Integrations** section on the main page.
5. Choose **Microsoft Outlook** as your integration.
6. On the **Add Outlook integration page**, enter the **Name** of your integration. This is the display name for the integration resource in AWS.
7. Add a **description** (optional).

8. In the **Workspace** section, enter your Microsoft **Tenant ID**. This can be found in the *Microsoft Entra Admin Center*. For more information, see How to find your tenant ID - Microsoft Entra
9. Choose the type of **Service access** method that you want the Outlook integration to use as authorization while accessing your service. You can **Create a new service role** or **Use an existing service role**. For more information, see IAM role for allowing the integration to call Amazon Q Business on your end user's behalf.
10. Choose the **Access management access** for the Outlook integration to authorize to connect to IAM Identity center. For more information, see IAM role for allowing Amazon Q Business to monitor the resources that the integration creates in your account.
11. Optionally, add any **Tags** that are relevant for this Teams integration.
12. Choose **Add integration**.
13. Once you have added the integration, Amazon Q will deploy your integration. You will see that update on the **Integration details page**.

    Once the integration is *deployed*, choose the name of your Outlook integration from the list of integrations in the **Integrations** section.
14. Copy the **Manifest URL** in the **Integration details** section.

    > **Note**
    >
    > You will now continue the remainder of this procedure within the *Microsoft 365 admin center*.

15. In the Microsoft 365 admin center, choose **Integrated apps** from the left navigation and choose **Upload custom apps** This will open the **Deploy New App** page.
16. Choose **Office Add-in** as your App type.
17. Paste the manifest URL link you copied in the **Provide link to manifest file** and choose **Validate**.
18. Choose the users you want to add in the **Add users** section.
19. Choose **Accept permissions** in the **Accept permissions requests** section and deploy the Add-in. Once deployment is completed, you users will be able to install the Amazon Q Business Add-in in their Microsoft Outlook.

> **Note**
>
> Authentication may be required.

Removing the Amazon Q Business Add-in as a Microsoft Outlook integration

To remove the Microsoft Outlook (Outlook) integration, Admin users can use the Amazon Q Business console.

> **Note**
>
> This integration can only be added using the Amazon Q Business console.

Using the console

1. Sign in to the Amazon Q Business console.
2. Choose **Applications**, then select the name of your application environment from the list.
3. Choose **Integrations** under **Enhancements**.
4. Choose your integration from the list in the **Integrations** section and choose **Delete**. Confirm your choice and choose **Delete**.

   > **Note**
   >
   > You will now continue the remainder of this procedure within the *Microsoft 365 admin center*.

5. Once your integration has been deleted, login to the Microsoft 365 admin center and choose **Integrated apps** from the left navigation.
6. Choose Amazon Q Business **Office Add-in** as your App and choose **Remove app** from the Amazon Q Business property details section that pops up. **Confirm** your choice.

> **Note**
>
> Once you remove your Microsoft Outlook (Outlook) Add-in from here, the Add-in will no longer appear as an Add-in to use or add in their Outlook.

Using the Amazon Q Business Add-in for Microsoft Outlook

Topics

- Prerequisites
- Install the Amazon Q Business Add-in to your Microsoft Outlook Install the Add-in
- Common use cases for using the Amazon Q Business Add-in for Microsoft Outlook
- Considerations for using the Amazon Q Business Add-in for Microsoft Outlook
- Troubleshooting the Amazon Q Business Add-in for Microsoft Outlook

Prerequisites

- You must have an Amazon Q Business user subscription.
- You must have a Microsoft 365 Business subscription.
- Your Amazon Q admin must add the Amazon Q Business Add-in to your Microsoft 365 organization.

Install the Amazon Q Business Add-in to your Microsoft Outlook

Install the Amazon Q Business Add-in to your Microsoft Outlook

The following are instructions on how to install the Amazon Q app in Microsoft Outlook (Outlook):

1. Open your Microsoft Outlook.
2. Go to **Add-Ins** and search for *Amazon Q Business* and choose **Amazon Q Business**
3. You will now see a **Q** icon/logo on the top bar on the right where you can access the Amazon Q Business chat assistant.
4. Once you have successfully logged on, you can use your Amazon Q Business Add-In.

Common use cases for using the Amazon Q Business Add-in for Microsoft Outlook

The following are some of the common use cases that will help you make the best use of your Amazon Q Business Add-in for Microsoft Outlook (Outlook):

1. **Analyze email threads**: Get summaries of long email discussions and identify key points, decisions, and action items.
2. **Draft email responses**: Select an email thread and ask Amazon Q to help draft appropriate responses based on the conversation context.
3. **Ask questions about email content**: Select any portion of an email thread and add it to the context, then ask your question. You can include multiple emails to provide more context.
4. **Ask a question about Amazon Q's company knowledge and general** (if enabled).
5. **Generate email content**: Describe what you need, and Amazon Q will generate suggested email content that matches the conversation's tone and context.
6. **Analyze up to 4 files that you want to send or have received for (collective) analysis**.

Considerations for using the Amazon Q Business Add-in for Microsoft Outlook

1. Amazon Q Business does not use customer data for service improvement or for improving its underlying large language models (LLMs). Also, none of the data you include in your Microsoft Outlook (Outlook) conversations will be indexed into your company's Amazon Q Business instance. For more information, see Amazon Q Business Service improvement.
2. To reset your conversation context, choose *new chat*. If you close the Amazon Q Business chat panel it will end the conversation and will start a new conversation the next time you reopen it.
3. All conversations with Amazon Q including uploaded web page snapshots and files from the Outlook will be deleted after 30 days of inactivity.
4. You can access all history of previous conversations (including attachments to those conversations) that have not been deleted from the Amazon Q web experience conversation history.
5. Amazon Q's responses aren't always 100% accurate. For more information, see Hallucination in the topic Key concepts of Amazon Q Business.

Troubleshooting the Amazon Q Business Add-in for Microsoft Outlook

- **My admin has enabled the Microsoft Outlook (Outlook), but I'm unable to login.**

Try having a conversation on your Amazon Q web experience first and then try the Microsoft Outlook (Outlook) again. If this doesn't work, then contact your Amazon Q admin or IT department.

- **Amazon Q doesn't respond helpfully or doesn't use the context of my email or document.**

  Try starting a new chat. If it still does not work, submit feedback using the feedback button and include any non-confidential details about the type of web page where the extension failed.

- **I get the error, 'To use the Amazon Q Business Add-in your administrator needs to enable "Allow end users to send queries directly to the LLM" in the Amazon Q Business console'**.

  Contact your Admin or IT department with the error.

- **Amazon Q doesn't recognize updated information when my thread updates.**

  Amazon Q only has access to your email thread right at the point you are viewing it. Similar to a photograph, this is all the information in the email thread is from the point it is viewed. To refresh the snapshot of your thread, go to the latest message in the thread.

Integrating Microsoft Word with the Amazon Q Business Add-in

Amazon Q Business can enhance your users' Microsoft Word (Word) experience by increasing their productivity, bringing Amazon Q's AI-powered assistance directly into their daily document workflows. As your users work on their documents, the Amazon Q Add-in can answer questions, review documents, suggest revisions and get insights from documents it has access to or from its general knowledge enhancing your users' productivity by bringing Amazon Q's AI-powered assistance directly into their document workflows.

With the Amazon Q Word Add-in your users can:

- Review, draft, and revise documents
- Summarize documents and get insights
- Simplify and improve your writing
- Access Amazon Q's company knowledge and general knowledge
- Upload documents and use other features available in the Amazon Q web experience.

Topics

- Configuring the Amazon Q Business Microsoft Word Add-in for use
- Removing the Amazon Q Business Add-in as a Microsoft Word integration
- Using the Amazon Q Business Add-in for Microsoft Word

Configuring the Amazon Q Business Microsoft Word Add-in for use

Note

- The Amazon Q Business customer integrating Microsoft Word (Word) must have a paid Word organization.
- Amazon Q supports users who authenticate using external SAML providers through IAM Identity Center. For more information, see Create an IAM Identity Center-integrated application.
- Amazon Q application environment created with IAM federation does not support the Word Add-in.
- Access using the Amazon Q Business API is not supported at this time.
- Amazon Q Business does not use user data for service improvement or for training its underlying large language models (LLMs). For more information, see Amazon Q Business Service improvement.
- Uploading documents and conversations will follow the same behavior as the web experience. For more information, see the Chat and file uploads section in the Using web experience topic.

Topics

- Prerequisites for integrating the Amazon Q Microsoft Word Add-in
- Integrating Microsoft Word with theAmazon Q Business Add-in

Prerequisites for integrating the Amazon Q Microsoft Word Add-in

As admins, before you can integrate the Amazon Q Business Microsoft Word (Word) Add-in, you must complete the following steps.

1. You must have a Microsoft 365 Business subscription and be a *Global Admin* or someone with administrative permissions, specifically `AppCatalog.ReadWrite.All`.

2. You need your Microsoft 365 tenant ID. For more information, see How to find your tenant ID - Microsoft Entra in the *Microsoft Learn portal*.
3. Get started with Amazon Q Business
4. Create an IAM Identity Center-integrated application and create your Amazon Q Business web experience.

> **Note**
>
> IAM federated application environments do not support integrations with Word.

5. Add the two IAM roles and trust policies for adding integrations. For more information, see IAM roles and trust policy for your integrations.
6. To use this feature, you must enable **Allow end users to send queries directly to the LLM** in your Admin controls and guardrails. For more information, see the Response settings topic in Admin controls and guardrails and `chatMode` if you are configuring programmatically.

Integrating Microsoft Word with theAmazon Q Business Add-in

To use the Amazon Q Business Add-in for Microsoft Word, you must allow it to connect to your Amazon Q Business application environment and web experience.

> **Note**
>
> This integration can only be added using the Amazon Q Business console.

Using the console

1. Sign in to the Amazon Q Business console.
2. Choose **Applications**, then select the name of your application environment from the list.
3. Choose **Integrations** under **Enhancements**.
4. Choose **Add integration** from the **Integrations** section on the main page.
5. Choose **Word** as your integration.
6. On the **Add Word integration page**, enter the **Name** of your integration. This is the display name for the integration resource in AWS.
7. Add a **description** (optional).

8. In the **Workspace** section, enter your Microsoft **Tenant ID**. This can be found in the *Microsoft Entra Admin Center*. For more information, see How to find your tenant ID - Microsoft Entra
9. Choose the type of **Service access** method that you want the Word integration to use as authorization while accessing your service. You can **Create a new service role** or **Use an existing service role**. For more information, see IAM role for allowing the integration to call Amazon Q Business on your end user's behalf.
10. Choose the **Access management access** for the Word integration to authorize to connect to IAM Identity center. For more information, see IAM role for allowing Amazon Q Business to monitor the resources that the integration creates in your account.
11. Optionally, add any **Tags** that are relevant for this Teams integration.
12. Choose **Add integration**.
13. Once you have added the integration, Amazon Q will deploy your integration. You will see that update on the **Integration details page**.

    Once the integration is *deployed*, choose the name of your Word integration from the list of integrations in the **Integrations** section.
14. Copy the **Manifest URL** in the **Integration details** section.

> **Note**
>
> You will now continue the remainder of this procedure within the *Microsoft 365 admin center*.

15. In the Microsoft 365 admin center, choose **Integrated apps** from the left navigation and choose **Upload custom apps** This will open the **Deploy New App** page.
16. Choose **Office Add-in** as your App type.
17. Paste the manifest URL link you copied in the **Provide link to manifest file** and choose **Validate**.
18. Choose the users you want to add in the **Add users** section.
19. Choose **Accept permissions** in the **Accept permissions requests** section and deploy the Add-in. Once deployment is completed, you users will be able to install the Amazon Q Business Add-in in their Microsoft Word.

> **Note**
>
> Authentication may be required.

Removing the Amazon Q Business Add-in as a Microsoft Word integration

To remove the Microsoft Word (Word) integration, Admin users can use the Amazon Q Business console.

> **Note**
>
> This integration can only be added using the Amazon Q Business console.

Using the console

1. Sign in to the Amazon Q Business console.
2. Choose **Applications**, then select the name of your application environment from the list.
3. Choose **Integrations** under **Enhancements**.
4. Choose your integration from the list in the **Integrations** section and choose **Delete**. Confirm your choice and choose **Delete**.

   > **Note**
   >
   > You will now continue the remainder of this procedure within the *Microsoft 365 admin center*.

5. Once your integration has been deleted, login to the Microsoft 365 admin center and choose **Integrated apps** from the left navigation.
6. Choose Amazon Q Business **Office Add-in** as your App and choose **Remove app** from the Amazon Q Business property details section that pops up. **Confirm** your choice.

> **Note**
>
> Once you remove your Microsoft Word (Word) Add-in from here, the Add-in will no longer appear as an Add-in to use or add in their Word.

Using the Amazon Q Business Add-in for Microsoft Word

Topics

- Prerequisites
- Install the Amazon Q Business Add-in to your Microsoft Word Install the Add-in
- Common use cases for using the Amazon Q Business Add-in for Microsoft Word
- Considerations for using the Amazon Q Business Add-in for Microsoft Word
- Troubleshooting the Amazon Q Business Add-in for Microsoft Word

Prerequisites

- You must have an Amazon Q Business user subscription.
- You must have a Microsoft 365 Business subscription.
- Your Amazon Q admin must add the Amazon Q Business Add-in to your Microsoft 365 organization.

Install the Amazon Q Business Add-in to your Microsoft Word

Install the Amazon Q Business Add-in to your Microsoft Word

The following are instructions on how to install the Amazon Q app in Microsoft Word (Word):

1. Open your Microsoft Word.
2. Go to **Add-Ins** and search for *Amazon Q Business* and choose **Amazon Q Business**
3. You will now see a **Q** icon/logo on the top bar on the right where you can access the Amazon Q Business chat assistant.
4. Once you have successfully logged on, you can use your Amazon Q Business Add-In.

Common use cases for using the Amazon Q Business Add-in for Microsoft Word

The following are some of the common use cases that will help you make the best use of your Amazon Q Business Add-in for Microsoft Word (Word):

1. **Review your document**: Select the text you want to review and get suggestions for improving clarity, grammar, and style.
2. **Summarize the document/generate content**: Open the Amazon Q Business add-in when reviewing a document and click on the **executive summary**, or **generate conclusion** quick prompts
3. **Ask questions about your content**: Select any portion of your document and add it as context, and ask your question. You can select multiple sections to provide more context or use quick prompts such as **explain in simple terms**.
4. **Simplify your content**: Select any portion of your document and ask your question. You can select multiple sections to provide more context or use quick prompts such as **simplify writing**.
5. **Generate content suggestions**: Select where you want to add content, describe what you need, and Amazon Q will generate suggestions that match your document's style and context.
6. **Draft your document or improve sections of your document:** Describe what you need, and Amazon Q will generate suggested draft content that matches the context.
7. **Ask a question about Amazon Q's company knowledge and general knowledge** (if enabled).
8. **Analyze up to 4 files that you want to review, summarize, or get insights from for (collective) analysis**.

Considerations for using the Amazon Q Business Add-in for Microsoft Word

1. Amazon Q Business does not use customer data for service improvement or for improving its underlying large language models (LLMs). Also, none of the data you include in your Microsoft Word (Word) conversations will be indexed into your company's Amazon Q Business instance. For more information, see Amazon Q Business Service improvement.
2. To reset your conversation context, choose *new chat*. If you close the Amazon Q Business chat panel it will end the conversation and will start a new conversation the next time you reopen it.
3. All conversations with Amazon Q including uploaded web page snapshots and files from the Word will be deleted after 30 days of inactivity.

4. You can access all history of previous conversations (including attachments to those conversations) that have not been deleted from the Amazon Q web experience conversation history.
5. Amazon Q's responses aren't always 100% accurate. For more information, see Hallucination in the topic Key concepts of Amazon Q Business.

Troubleshooting the Amazon Q Business Add-in for Microsoft Word

- **My admin has enabled the Microsoft Word (Word), but I'm unable to login.**

  Try having a conversation on your Amazon Q web experience first and then try the Microsoft Word (Word) again. If this doesn't work, then contact your Amazon Q admin or IT department.
- **Amazon Q doesn't respond helpfully or doesn't use the context of my email or document.**

  Try starting a new chat. If it still does not work, submit feedback using the feedback button and include any non-confidential details about the type of web page where the extension failed.
- **I get the error, 'To use the Amazon Q Business Add-in your administrator needs to enable "Allow end users to send queries directly to the LLM" in the Amazon Q Business console'.**

  Contact your Admin or IT department with the error.

IAM roles and trust policy for your integrations

In order for your integrations to work, you will need to add the following two IAM roles as part of your configuration.

> **Note**
>
> IAM roles and trust policy are not required for using browser extensions.

Topics

- IAM role for allowing the integration to call Amazon Q Business on your end user's behalf
- IAM role for allowing Amazon Q Business to monitor the resources that the integration creates in your account
- IAM trust policy for your integrations

IAM role for allowing the integration to call Amazon Q Business on your end user's behalf

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessConversationPermissions",
            "Effect": "Allow",
            "Action": [
                "qbusiness:Chat",
                "qbusiness:ChatSync",
                "qbusiness:PutFeedback",
                "qbusiness:DeleteConversation",
                "qbusiness:ListAttachments",
                "qbusiness:DeleteAttachment"
            ],
            "Resource": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
        },
        {
            "Sid": "QBusinessKMSDecryptPermissions",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/[[key_id]]"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "qbusiness.us-east-1.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "QBusinessSetContextPermissions",
            "Effect": "Allow",
```

```
            "Action": [
                "sts:SetContext"
            ],
            "Resource": [
                "arn:aws:sts::*:self"
            ],
            "Condition": {
                "StringLike": {
                    "aws:CalledViaLast": [
                        "qbusiness.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

IAM role for allowing Amazon Q Business to monitor the resources that the integration creates in your account

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessIdCInstanceReadOnlyPermissions",
            "Effect": "Allow",
            "Action": [
                "sso:ListApplications"
            ],
            "Resource": "arn:aws:sso:::instance/idc-instance-id"
        },
        {
            "Sid": "QBusinessIdCInstanceApplicationReadOnlyPermissions",
            "Effect": "Allow",
            "Action": [
                "sso:ListApplicationAccessScopes",
                "sso:GetApplicationAssignmentConfiguration",
                "sso:GetApplicationGrant",
                "sso:GetApplicationAuthenticationMethod"
```

```
            ],
            "Resource": "arn:aws:sso::111122223333:application/idc-instance-id/*"
        }
    ]
}
```

IAM trust policy for your integrations

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessTrustPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "integrations.qbusiness.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
                }
            }
        }
    ]
}
```

Creating purpose-built *Amazon Q Apps*

Important

As of July 1, 2024, Amazon Q Apps are available only to Amazon Q Business Pro users. Amazon Q Business Lite users will no longer be able to create, run, or view Q Apps. To access, Q Apps, Lite users must upgrade to Amazon Q Business Pro.
As of August 30, 2024, all Amazon Q Apps created by Lite users who did not upgrade their account to Amazon Q Business Pro have been deleted.

You and your web experience users can create lightweight, purpose-built *Amazon Q Apps* within your broader Amazon Q Business application environment. Using your enterprise data, users can create a generative AI-powered app that streamlines their tasks. These Q Apps can be easily created by anyone at the click of a button, transforming their conversations with an Amazon Q Business assistant into reusable and shareable Amazon Q Apps.

Teams across your organization can create Amazon Q Apps tailored to their specific workflows and business needs. When your Amazon Q Business assistant generates useful content, users can transform those conversations into reusable apps that automate repetitive tasks and ensure consistency. The following examples show how different teams might use Amazon Q Apps:

Example Marketing content generator

A marketing team member creates a Amazon Q App that generates social media posts following company branding guidelines. The app includes:

- Input card: Product name and key features
- Text output card: Generates professional post with company tone
- Text output card: Creates social-media-friendly version

Result: Team members can quickly generate consistent branded content for any product launch.

Example Employee onboarding assistant

An HR team creates a Amazon Q App to streamline new employee setup:

- Input card: Employee name, department, start date
- Plugin card: Creates Jira ticket for IT equipment setup

- Text output card: Generates personalized welcome email
- File upload card: Processes signed documents

Amazon Q Apps is enabled by default when you create a new Amazon Q Business application environment using IAM Identity Center or IAM Federation in the Amazon Q Business console. Amazon Q Apps can be accessed through the web experience.

You can also create and manage Q Apps programmatically. For an more information, see Amazon Q Apps in the *Amazon Q Business API Reference*.

Topics

- Prerequisites for Amazon Q Apps
- Managing Amazon Q Apps
- Using the web experience to create and run Amazon Q Apps
- Sharing Amazon Q Apps
- Custom labels for Amazon Q Apps
- Understanding and managing Verified Amazon Q Apps
- Data collection in Amazon Q Apps
- Using plugins in Amazon Q Apps

Prerequisites for Amazon Q Apps

Before using Amazon Q Apps, make sure that you do the following:

- **Set up your identity provider** – For web experience users to create and run their own Amazon Q Apps within a broader Amazon Q Business application environment, they must be recognized by either IAM Identity Center or AWS Identity and Access Management (IAM). These users can continue to authenticate either directly through IAM Identity Center, or through an existing enterprise identity provider connected to IAM Identity Center or IAM (like Okta, Microsoft Entra ID, and Ping Identity, among others). When users attempt to use an Amazon Q Business web experience, Amazon Q Apps authorizes their actions based on the user and group information it gathers from IAM Identity Center or IAM.

  To set up IAM Identity Center, see Enable single sign-on access to your AWS applications (Application admin role) in the *IAM Identity Center User Guide* . You need to complete this step before creating an Amazon Q Business application environment and using Amazon Q Apps. For

a list of supported enterprise identity providers and how to connect them to your IAM Identity Center instance, see Manage an external identity provider in the *IAM Identity Center User Guide*.

To set up AWS Identity and Access Management, see Get started with IAM in the *AWS Identity and Access Management User Guide*. You need to complete setting up and connecting an identity provider to an IAM instance before creating an Amazon Q Business application environment and using Amazon Q Apps. For a list of supported enterprise identity providers and how to connect them to your IAM instance, see Identity providers and federation in the *AWS Identity and Access Management User Guide*. For an example of how to set up an Amazon Q Business application environment with IAM federation using Okta as an example, see Configuring an Amazon Q Business application using IAM Federation.

> **Important**
>
> As of July 1, 2024, Amazon Q Apps are available only to Amazon Q Business Pro users. Amazon Q Business Lite users will no longer be able to create, run, or view Q Apps. To access, Q Apps, Lite users must upgrade to Amazon Q Business Pro.
> As of August 30, 2024, all Amazon Q Apps created by Lite users who did not upgrade their account to Amazon Q Business Pro have been deleted.

- **Finish the Amazon Q Business setup** – Complete setting up Amazon Q Business and create an Amazon Q Business application environment integrated with either IAM Identity Center or AWS Identity and Access Management. Configuring the application environment is necessary so that you can allow users to manage their own Amazon Q Apps. Also, include a retriever and, optionally, a data source connector.
- **Create an IAM role** – Configure an AWS Identity and Access Management (IAM) access role (permissions policy) for the deployed web experience for your broader application environment, including permissions for Amazon Q Apps. The admin can use the Amazon Q Business console to create the required IAM role for users as part of the configuration steps. To view and modify the required IAM access role with set permissions and optional permissions for web experience users to view and specify approved data sources with Amazon Q Apps, see the IAM role for web experience users.

> **Note**
>
> If you are using permissions for Amazon Q Apps created prior to July 10, 2024, you must update your role with the new Amazon Q Apps permissions for your users to have

access to use the permissions to view and specify approved data sources and other future features in Q Apps.

- **Quotas** *(formerly known as limits)* — There are set maximum quotas for Amazon Q Apps. For information about these quotas, see Quotas.

Managing Amazon Q Apps

You can enable or disable the ability for web experience users to create and run their own Amazon Q Apps. To do this, use the feature settings for your broader application environment, as part of the admin controls and guardrails in the Amazon Q Business console.

You can also manage Amazon Q Apps through the console. You can view the list of all published Q Apps created within your broader application environment. To do this, select your application environment's *name* and then go to **Amazon Q Apps** in the navigation menu. From this list, you can remove one or more published apps from your library of Amazon Q Apps.

Using the web experience to create and run Amazon Q Apps

After you enable Amazon Q Apps in the console, web experience users can then start creating, running, and publishing their own purpose-built Q Apps.

Within the Amazon Q Business web experience, users can create an Amazon Q App from an existing conversation or prompt. Users can simply generate Q Apps in a single step from their conversation with Amazon Q Business or by describing their requirements using natural language prompts.

To use the Amazon Q Business web experience, users must be granted access using IAM Identity Center. You share the endpoint URL of your web experience page with your users, who go to the URL and are authenticated to access the web experience. This endpoint URL is in the **web experience settings** of your application environment in the Amazon Q Business console. To create and run Amazon Q Apps, users go to the web experience endpoint URL and then select **Apps** from the navigation menu.

For users to create an Q App from a conversation, once in a conversation, they can choose the **Create Amazon Q App** button to transform it into an app for use.

Within **Apps**, users can try the example prompts by selecting the **Amazon Q Apps Creator** in the web experience. Users can create, edit, run, publish, and delete their apps. Users can also directly

create an app by describing their requirements using natural language prompts in the **Amazon Q Apps Creator**.

An Amazon Q App is made up of a collection of cards. A card is a UI element in the web experience that users can combine with other cards to create an app. Cards take a users' inputs, support file uploads, connect to other cards, generate text outputs, and allow actions through new and legacy Amazon Q Business built-in plugins and Amazon Q Business custom plugins (if activated), from within Q Apps. Users can select their Amazon Q App to add, edit, or delete a card.

> **Note**
>
> For tips on using effective prompting with Amazon Q Apps, see this Community Article on AWS re:Post.

Text output and plugin cards contain *prompt* instructions that determine how Amazon Q Business is queried to generate a response. When your users use the **Amazon Q Apps Creator**, relevant cards are auto-generated with pre-filled prompts. Your users can further refine these prompts using simple, natural language. When writing or editing a prompt for a card, users can reference other cards using an *@ mention* to select a card from the list of cards in the app.

Users can also instruct the cards to reference your enterprise data in Amazon Q Business or, they can specify a data source from a list of your available *data sources* (requires additional IAM permissions from the admin). This allows users to focus the Q App's output on a particular subset of your data, rather than querying across the entire index. For example, an app that is built to summarize weekly sales updates by geography can have the output cards with results from the data source tied to a specific geography, rather than your company's entire data repository or the LLM's foundational knowledge.

Users can then share the Amazon Q Apps that they have created with other web experience users. To do this, they open their Amazon Q App and then choose **Publish** to share it with other users through your company's Amazon Q Apps library. When you publish an app, you can also assign helpful labels to it to make them easier to group my subject matter or purpose.

To have your published Q Apps become *Verified*, you'll need to work with your Amazon Q Business administrators. Admins can review your published apps and update the status to *Verified* if they determine the app meets your organization's criteria. When users access the Q Apps Library, they will see a distinct blue checkmark icon on any apps that have been marked as **Verified** by

administrators. Verified apps are automatically surfaced to the top of the app list within each category, making them easily discoverable. . For more information, see Understanding and managing Verified Amazon Q Apps

Published Amazon Q Apps are made available in the your Amazon Q Apps library. The creator of an app can edit their own Amazon Q App and publish changes. This updates the app in the library. Other users can copy and customize a published Amazon Q App and create a new version. However, other users cannot edit the original app, only the creator can. Users can also show their support for a useful Amazon Q App by selecting the like button for the app in the library.

> **Note**
>
> If you update an Amazon Q App with a verified label, it will lose its verified status until the admin re-applies the label. Maintaining an app's *Verified* state requires ongoing collaboration with your administrators.

Sharing Amazon Q Apps

Amazon Q Apps allows you to privately share your Q Apps with specific users within your Q Business application environment. This private sharing capability enables app creators to restrict app access to select users, providing more granular control over app visibility and usage within organizations.

Benefits

- **Controlled Access**: Share your Q Apps with only the intended users, maintaining privacy and security.
- **Run-Only Mode**: Shared users can view and run the Q App but cannot make structural changes. To make structural changes, they will first need to duplicate it, which creates their separate, editable copy of the Q App.

Key Concepts

- Owner: The owner is the user who creates and has full editing rights over the Q App. As the owner, you can:
  - Privately share the Q App with other users by full email address.

- Revoke access for shared users.
- Edit the category for the shared Q App, which affects where it appears in the shared app user's library.

- App User: A shared app user is a user within your organization's Q Business environment that the owner has shared the Q App with by email. As a shared user, you can:
  - View and run the shared Q App.
  - Duplicate the Q App to create an editable version.
  - Cannot directly edit the original shared Q App.

Shared users do not receive a notification when a Q App is shared with them. You need to send them the link from the share modal.

Prerequisites for Private Sharing

Before your web experience users can use sharing you will need to update the web experience IAM role to enable private sharing in the web experience. We recommend updating the `DescribeQAppPermissions` `UpdateQAppPermissions` statement of the IAM policy attached to this role to include the action as follows:

```
{
    "Sid": "QAppsAppOwnerPermissions",
    "Effect": "Allow",
    "Action": [
        "qapps:GetQApp",
        "qapps:CopyQApp",
        "qapps:UpdateQApp",
        "qapps:DeleteQApp",
        "qapps:ImportDocument",
        "qapps:ImportDocumentToQApp",
        "qapps:CreateLibraryItem",
        "qapps:UpdateLibraryItem",
        "qapps:StartQAppSession",
        "qapps:DescribeQAppPermissions",
        "qapps:UpdateQAppPermissions"
    ],
    "Resource": "arn:aws:qapps:{{region}}:{{source_account}}:application/
{{application_id}}/qapp/*",
    "Condition": {
```

```
        "StringEqualsIgnoreCase": {
            "qapps:UserIsAppOwner": "true"
        }
    }
}

{
    "Sid": "QAppsPublishedAppPermissions",
    "Effect": "Allow",
    "Action": [
        "qapps:GetQApp",
        "qapps:CopyQApp",
        "qapps:AssociateQAppWithUser",
        "qapps:GetLibraryItem",
        "qapps:CreateLibraryItemReview",
        "qapps:AssociateLibraryItemReview",
        "qapps:DisassociateLibraryItemReview",
        "qapps:StartQAppSession",
        "qapps:DescribeQAppPermissions"
    ],
    "Resource": "arn:aws:qapps:{{region}}:{{source_account}}:application/
{{application_id}}/qapp/*",
    "Condition": {
        "StringEqualsIgnoreCase": {
            "qapps:AppIsPublished": "true"
        }
    }
}
```

Sharing Amazon Q Apps

Web Experience

To privately share your Q App

1. Open the Q App you want to share.
2. Choose on the "Share" button in the top right corner.
3. In the share modal, enter the email addresses of the users you want to share with, or you can toggle ‘Share with all’ to give access to everyone in your Q Apps organization.
4. Edit the category(s) for the shared Q App, which affects where it appears in the shared user's library.

5. (Optional) Choose the copy icon to obtain the link; this can then be sent to shared users via your preferred method (e.g., email or Slack).
6. Choose "Share" to complete the sharing process.

The shared users will now be able to access and run your Q App from the library or via the shareable link you provide them.

AWS CLI

To privately share your Q App with AWS CLI, use the `DescribeQAppPermissions` command.

```
aws qapps describe-q-app-permissions \
            --instance-id instanceId \
            --app-id appId
```

Managing Shared Users

As the owner, you can manage who has access to your shared Q App by revisiting the share modal:

Web Experience

1. To revoke access, choose the "Remove" button next to the user's email address.
2. To grant access to new users, enter their email addresses.
3. Choose "Share" to apply the changes.

AWS CLI

To manage share user access with AWS CLI, use `UpdateQAppPermissions`.

```
aws qapps update-q-app-permissions \
            --instance-id instanceId \
            --app-id appId \
            --grant-permissions listOfPermissions to be granted \
            --revoke-permissions listOfPermissions to be revoked \
```

Custom labels for Amazon Q Apps

To organize and classify apps based on your unique business needs, Administrators can customize the labels available for published Q Apps. You can add up to 10 labels, and remove or update existing labels. Labels help web experience users find Q Apps in the library.

For example, you might add custom HR organization-specific labels like *Employee onboarding* and *Benefits inquiries*. When members of your HR team create and use Q Apps, they can use these labels to classify them and help other users find the apps they need.

Topics

- Prerequisites for customizing labels
- Considerations for customizing labels
- Customizing labels

Prerequisites for customizing labels

Before your web experience users can use custom labels, the web experience IAM role for your application environment must have permission to perform the `qapps:ListCategories` action. We recommend updating the `QAppsResourceAgnosticPermissions` statement of the IAM policy attached to this role to include the action as follows:

```
{
"Sid": "QAppsResourceAgnosticPermissions",
"Effect": "Allow",
"Action": [
    "qapps:CreateQApp",
    "qapps:PredictQApp",
    "qapps:PredictProblemStatementFromConversation",
    "qapps:PredictQAppFromProblemStatement",
    "qapps:ListQApps",
    "qapps:ListLibraryItems",
    "qapps:CreateSubscriptionToken"
    "qapps:ListCategories"
],
"Resource": "arn:aws:qbusiness:us-west-2:account-number:application/application-id"
}
```

Considerations for customizing labels

When you add labels, note the following:

- The maximum number of labels for an application environment is 10. This includes predefined labels.
- You can't add duplicate labels.
- Labels can't include special characters.

Customizing labels

To customize labels available in an application environment for Q Apps, you can use the Amazon Q Business console or the following API operations.

- ListCategories
- BatchUpdateCategory
- BatchCreateCategory
- BatchDeleteCategory

After you save your changes, the label updates appear in the web experience immediately. If users don't see the changes, make sure you have configure permissions for the web experience IAM role for your application environment correctly. For more information, see Prerequisites for customizing labels.

The following shows how to customize Q Apps with the Amazon Q Business console or the AWS Command Line Interface.

Console

To customize labels for Q Apps, navigate to the **Q Apps** page for your application environment, choose the **Settings** tab, and add, update, or remove labels.

To customize labels

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, choose the name of your application environment from the list of applications.

3. From the left navigation menu, choose **Enhancements**, and then choose **Amazon Q Apps**.
4. Choose the **Settings** tab, and add, update, or remove labels.
5. Choose **Save**. After you save your changes, the label updates appear in the web experience immediately.

AWS CLI

To customize labels with the AWS CLI, use the `list-categories`, `batch-update-category`, `batch-create-category` or `batch-delete-category`commands.

- To view all custom labels for your application environment, use the `list-categories` command.

```
aws qapps list-categories --instance-id instanceId --region region
```

- If you have reached the 10 label limit, you can use the `batch-update-category` command to update an existing category name.

```
aws qapps batch-update-category \
--instance-id instanceId \
--categories '[{"id":"existingCategoryId","title":"updatedCategoryName"}]' \
--region region
```

- If you have less than 10 labels, you can use the `batch-create-category` command to add new labels.

```
aws qapps batch-create-category \
--instance-id  instanceId \
--categories '[{"id":"uniqueId","title":"newCategoryName"}]' \
--region region
```

- To delete categories, use the `batch-delete-category` command. For `categories`, specify the list of IDs of the categories to be deleted.

```
aws qapps batch-delete-category \
--instance-id instanceId \
--categories '["categoryId1", "categoryId2"]' \
--region region
```

Understanding and managing Verified Amazon Q Apps

The Verified Q Apps feature empowers administrators to endorse published Amazon Q Apps. The goal is to enhance governance and provide a clear signal to end-users about which Q Apps are recommended for use within their organization. By labeling apps as *Verified*, admins can help improve trust and adoption of the most valuable, high-quality Q Apps created by employees.

Admins can easily endorse published Q Apps by updating their status from *Default* to *Verified* directly within the Amazon Q Business console. The idea is that admins would work closely with their business stakeholders to determine the criteria for verifying apps, based on their organization's specific needs and policies. This admin-led labeling capability is a reactive approach to endorsing published apps, without gating the publishing process for app creators.

When users access the Amazon Q Apps Library, they will see a distinct blue checkmark icon on any apps that have been marked as *Verified* by administrators. Additionally verified apps are automatically surfaced to the top of the app list within each category, making them easily discoverable. Users can also filter the library to view only Verified apps.

> **Note**
>
> If a Amazon Q App is unpublished and then re-published, or if changes are made to a *Verified* app, the verified label will be removed until the administrator re-applies it.

Topics

- Considerations for verifying Amazon Q Apps
- Verifying Amazon Q Apps
- Restoring Amazon Q Apps to the default state

Considerations for verifying Amazon Q Apps

To start using the Verified Apps feature in Amazon Q Apps, consider the following:

- **Determine Verification Criteria:** Work with business stakeholders to establish the criteria for verifying Q Apps. This could include factors like content quality, alignment with organizational policies, and user feedback.
- **Review Published Apps:** Review the list of published apps against your criteria. This can be accessed from the Amazon Q Business console or API.

Verifying Amazon Q Apps

To update an app state to verified you can use the console; or the UpdateLibraryItem API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To verify Amazon Q Apps

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. From the left navigation menu, choose **Enhancements**, and then choose **Amazon Q Apps**.
4. In the **Amazon Q Apps in library** section, choose the Q Apps that you want to verify, and then choose **Update state**.
5. From the **Update state** drop down, choose **Verified**.

AWS CLI

To verify Amazon Q Apps

```
// to add the verified label
                        aws qapps update-library-item-metadata \
                        --instance-id  instanceId \
                        --library-item-id  libraryItemId \
                        --is-verified \
```

Restoring Amazon Q Apps to the default state

All Amazon Q Apps are always in a *Default* state when they are first published or updated. To remove an Amazon Q App verified state and change it back to default you can use the console; or the UpdateLibraryItem API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To restore Amazon Q Apps state to default

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. From the left navigation menu, choose **Enhancements**, and then choose **Amazon Q Apps**.
4. In the **Amazon Q Apps in library** section, choose the Q Apps that you want to verify, and then choose **Update state**.
5. From the **Update state** drop down, choose **Default**.

AWS CLI

To restore Amazon Q Apps state to default

```
// to add the verified label
                        aws qapps update-library-item-metadata \
                        --instance-id  instanceId \
                        --library-item-id  libraryItemId \
                        --no-is-verified \
```

Data collection in Amazon Q Apps

> **Note**
>
> The Amazon Q Apps data collection feature is in preview and is subject to change.

A data collection app is an Amazon Q App with one or more form cards that collect multiple pieces of information from app users. For example, you might use a data collection app to conduct team surveys, organize project retrospectives, collect ideas for next year's goals, or collect questions for a town hall. These apps can leverage generative AI to analyze the collected data, identify common themes, summarize ideas, and provide actionable insights.

When creating a data collection app, you add one or more data collection form cards. You can also add output cards that use generative AI to analyze or summarize participants' data. For each form card, you add one or more text input fields. For example, a user can submit an idea and the reason to prioritize. Forms can be configured to allow multiple submissions by the same user. For example, users can submit multiple ideas for next year's goals.

After you share your app, you and other users can open it and start collecting data. When anyone opens the app and starts a data collection, they become a data collection owner. An owner can own only one active data collection per app. More than one user can start a data collection for the same app. The data collection owner shares the data collection with participants, controls access to the forms and data collection results, and controls when to start and stop accepting submissions.

As the owner of a data collection, choose when reveal or hide the data from the form. For example, your app might collect ideas from the team for next year. Based on the collected data, you can choose to hold off on revealing the responses and any generative AI analysis or summaries.

Topics

- Permissions requirements
- Data collection concepts
- Creating a new Q App with a data collection form
- Starting a new data collection

Permissions requirements

For users to create and use data collection apps, the web experience IAM role for your Amazon Q Business environment must have the following permissions for session resources:

- qapps:GetQAppSessionMetadata
- qapps:UpdateQAppSessionMetadata
- qapps:ListQAppSessionData
- qapps:ExportQAppSessionData

For more information, including a policy example, see IAM permissions for using Amazon Q Apps.

Data collection concepts

This topic outlines specific concepts and features of Data collection forms in Amazon Q Apps. These concepts are key to understanding how to collect data from users with Amazon Q Apps.

Topics

- Data collection
- Data collection form

- Creator
- Data collection owner
- User
- Shareable link
- Access control and security

Data collection

A *data collection* is a pool of data that contains all participant responses submitted through the data collection form, as well as the configuration settings for how participants can access and submit data. Key aspects of data collections include the following:

- Instantiation – After you publish your data collection app to the library, other users can open it and create a data collection. When a user creates a data collection, they become the data collection owner. Each owner has a unique shareable link they use control over which users participate. There can be multiple data collections for a single app.
- Data isolation – Each data collection maintains its own separate pool of data. This ensures that each owner's data collection stays completely separate from any other owners' using the app.
- Access control – The data collection owner creates and shares unique access links with participants.
- Flexibility – Multiple owners can create data collections from the same data collection app. For example, you might have a Project Retrospective data collection app. Different owners can create new data collections for different projects from this same app.
- Owner control – The owner manages access and data collection configuration.

Data collection form

A *data collection form* is a unique Amazon Q Apps card type that allows you to collect multiple pieces of information from participating users. You can add up to 20 data collection form cards per app.

Creator

A *creator* is the user who designs and builds the Q App with the data collection form. Creators have the ability to do the following:

- Add data collection form cards.
- Define the form's fields.
- Set up and make changes to the overall structure of the Q App.
- Initiate data collections (i.e., operate as the 'owner' of the data collection app) of the Q App tow collect data from different groups of users.
- Can share, re-share, and unshare the Q App to and from the library.
- Creators can be owners of a data collection associated with their own app.

Data collection owner

An owner is a user who opens a data collection app and configures a new data collection with a shareable link. Owners control the data collection, including access and submission settings. They can own only one active data collection per app.

Key aspects of the Owner role include:

- Data collection management – Owners control the data collection, including when to start and stop accepting responses.
- Access control – Owners manage who can by access the data collection by sharing the link located in the data collection settings.
- Advanced settings – Owners can use the data collection's advanced settings to allow users to submit data or see all collected data. This is important when the data collection is being used for sensitive information (e.g., personal identifying information (PII)). For more information, see Access control and security.
- Limited app editing capabilities – They can't make structural changes to the core data collection app (i.e., add, edit, and remove cards).

User

A user accesses a shared data collection app via the unique data collection link provided by the owner to submit data. Key aspects of the user role include –

- Response submission – users can fill out and submit data using a form within the data collection.
- Limited access – users cannot modify the form structure or manage data collection data collection settings.

- Viewing data – Depending on controlled data collection settings, users may or may not be able to view other users' submissions.
- Multiple submissions – users may be able to submit multiple inputs, based on the form's configuration.

Shareable link

A shareable link is a unique URL that provides access to a specific data collection app. Owners share this link with intended participants over a channel of their preference, such as email or slack. Key features of shareable links include:

- Access control – Links are private and can only be accessed by users within the organization's Q Instance.
- Data collection-specific – Each link corresponds to a particular data collection of the Q App.
- Security – Links may have additional security measures, such as expiration dates or user authentication requirements.

Access control and security

The Data collection owner controls who can submit data and who can view the collected data.

Topics

- Data access
- Data visibility
- Multiple submissions
- Limitations
- Security

Data access

By default, the shareable data collection link allows anyone within your organization to submit data. As the owner, you can choose to:

- Leave the data collection open for unlimited submissions.
- Disable submissions at any time.

Data visibility

The visibility of submitted data is also controlled by the owner. By default, all users can view the collected data. You can choose to hide results and only reveal them when you're ready to review the data.

This flexibility allows you to control the data collection form process – whether you want it to be an open, transparent exercise or a more controlled, private exercise. The owner maintains full control over the data collection settings and data access. Users can only submit data through the shared data collection link and view data based on the owner's permissions.

Multiple submissions

By default, data collection forms limit users to one response. When you add a data collection form, you can clear the **Limit users to one response** check box to allow for multiple submissions from each user within a data collection. If a user submits a form multiple times in the same data collection, all of their submissions are be saved. If you use a single submission form, only the recent submission is saved.

Limitations

The following are limitations for data collection apps

1. Isolated data usage – The collected data is confined to the Q App where they're created. You cannot combine them with other data sources or use different card output types within the same app.
2. Optional form fields – By default, form fields aren't required. Users can submit forms without completing all fields, potentially resulting in incomplete data.
3. Number of data collection cards:Creators can add up to 20 data collection form cards to a single Q App.

Security

All data collected through Amazon Q Apps data collection form are stored securely within your organization's Q Instance and are not accessible to anyone outside your organization.

Creating a new Q App with a data collection form

To create a new data collection app, you create a new app, add a data collection form with one or more fields, and publish the app.

1. Go to your Amazon Q Business web experience URL.
2. In the navigation pane, choose **Apps**.
3. Choose one of four methods to start creating your Q App data collection form:

   - In **Recently used** choose the pencil icon.
   - Choose a tile that contains a **Data collection** pill
   - Describe your Q App data collection form use case in the text entry box and choose **Generate**.
   - Choose **Create blank app**
   - Choose **Explore the Q Apps library** to start with any existing apps your team may have already created and shared.
4. Choose **+ Add card** and choose **Data collection form**.
5. Choose the pencil icon on the data collection form.
6. For **Title**, give the form a name.
7. Under **Fields**, add one or more fields with field labels.

   - Choose **+ Add a field** to add more fields.
   - Choose the trash can icon to delete a field.
8. Choose **Save** to save the form.
9. Add any necessary output cards to analyze the collected data. Use `@cardname` to reference the data from the form card in the prompt.
10. When you are finished, the top right, choose **Share**.
11. Configure how you want to share the app and optionally edit its categories.
12. Choose **Share**. When complete, you can find the new app in your library.

Starting a new data collection

You can start a new data collection with the web experience or with the Q Apps APIs.

Web experience

To start a new data collection, you open an app with a data collection form, configure data collection settings, and then copy and share the link to start collecting responses.

1. Go to your Amazon Q Business web experience URL.

2. In the navigation pane, choose **Apps**.
3. Locate and open an existing Q App that has a data collection form.
4. Choose **Start data collection** at the top right.
5. Enter a name for the data collection. For example, John Doe's All-Hands Meeting. You use this name when you reference the data from the form in other cards. For example, outputting an AI-generated summary of responses to an output card in the app.
6. In **Advanced settings**, configure the participant experience with the **Allow users to submit data** and **Allow users to see all collected data** check boxes.
7. Choose **Create**.
8. Choose the options to enable/disable form submissions and whether users can see others' data.
9. Choose the **Copy** icon to obtain the shareable link.
10. Choose **Save**.
11. Share the link directly with your users. As users respond to questions, you can do the following from your app:

    - To see user data, on the form collection card, choose **All data**.
    - To delete collected data, choose **Data collection settings** and choose **Delete collected data**.
    - To stop or restart collecting data, toggle the **Allow users to submit data** check box.

Q Apps APIs

Owners can start and manage data collections with the following APIs:

- `StartQAppSession` - Start a new data collection.
- `UpdateQAppSessionMetadata` - Update metadata for the data collection. For example, give the collection a name.
- `UpdateQAppSession` - Optionally provide answers to your own data collection questions.
- `ListQppSessionData` - List all submitted values for form cards.
- `ExportQAppSessionData` - Export data in CSV format
- `StopQAppSession` - Terminate the session

For participants, use the following APIs:

- `StartQAppSession` - Associate the user with the data collection.
- `GetQAppSession` - Get the latest state of the data collection. Use this API before and after submitting data into form cards.
- `ListQAppSessionData` - Get all submitted values for form cards.
- `UpdateQappSession` - Submit data into form cards.

Using plugins in Amazon Q Apps

If plugins are configured for your Amazon Q Business application environment you can add these to a Amazon Q Apps you're creating. Once you add a plugin to your Q Apps, your app users will be able to perform plugin actions from within your Q Apps.

All plugins (new and legacy built-in plugins, and custom plugins) configured in the Amazon Q Business console will be available for Q App creators to use.

> **Important**
>
> You can add only one action per plugin card.

The following section outlines how to add plugins to your Q Apps using both the AWS Management Console and the AWS CLI.

Topics

- Prerequisites for adding plugins
- Adding plugins in Amazon Q Apps
- Using plugins in Amazon Q Apps

Prerequisites for adding plugins

Before your web experience users can create and use plugins, the web experience IAM role for your application environment must have the correct permissions to perform the necessary actions. We recommend updating your web experience IAM policy following the steps outlined in Prerequisites for configuring Amazon Q Business built-in plugins.

Adding plugins in Amazon Q Apps

To add a plugin to your Q App you can use either the AWS Management Console or the CreateQApp API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

> **Note**
>
> You can also add a plugin to your Q App through your Amazon Q Business web experience URL.

Console

To add a plugin card to an Q App

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. From the left navigation menu, choose **Enhancements**, and then choose **Amazon Q Apps**.
4. In the **Amazon Q Apps in library** section, choose the Q Apps that you want to add a plugin card to, and then select the web experience URL for that Q Apps.
5. From the Q Apps **App library** navigate to your app and select **Open**.
6. On the Q App page that opens, select **Add card**, and then select **Actions**.
7. From the **Actions** menu that opens up on the right, do the following:

   - For **Title** – Add a title for the card.
   - For **Plugin** – Select the plugin you want to add. Then, choose the actions you want your plugin to be able to perform.

     > **Note**
     >
     > You can only add one action per plugin card.

   - For **Prompt** – In the prompt section, you get a dropdown of actions for the plugin you select. Once you select an action in the dropdown, your prompt will be populated with a recommended template that you can use for configuration. We recommend that Q App

creators follow the generated prompt when writing their own prompts to achieve better results.

8. Select **Save**.

AWS CLI

To add a plugin to an Q App

```
// Create an app with a single plugin card
aws qapps create-q-app \
--title appTitle \
--instance-id qBusinessApplicationId \
--description pluginDescription \
--app-definition '{"cards":[{"qPlugin":{"type":"q-plugin","title":"Action
 Card","id":"cardUUID","pluginId":"QBusinessPluginId","actionIdentifier":"pa:jira:999.0_0:/
rest/api/2/issue:POST","prompt":"Create a task in my project"}}]}'
```

Using plugins in Amazon Q Apps

To use a plugin within a Q App you can use either the Amazon Q Business web experience URL or the StartQAppSession API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Web experience

To use a plugin in an Q App

1. From your **Q App** with plugins, select **Run**.

   A window will open up asking you to log in to your third party plugin account.

2. After you login, Q Apps displays a dialog box asking you to grant your Q App permission to access your third party plugin account. From the box, select **Allow**.

> **Note**
>
> If there are multiple plugins configured for a Q App, the authentication flow for the second app occurs after the first one.

3. After a successful connection, your plugin card will display a form where you can fill in the details for the action you are taking.
4. After filling in the details needed, select **Create**.

   Your plugin card displays a success message when your action completes successfully.

AWS CLI

To use a plugin in an Q App

```
// start execution of an app

aws qapps start-q-app-session \
--app-id fill in from create or get q app response \
--app-version fill in from create or get q app response \
--instance-id qBusinessApplicationId \


// If you have input cards that should be passed to the plugin:

aws qapps start-q-app-session \
--app-id fill in from create or get q app response \
--app-version fill in from create or get q app response \
--initial-values '{"cardId":"fill in from create q app input or get q app
 response","value":"fill in"}' \
--instance-id qBusinessApplicationId \


// To get the status of an app, and results (if any):

aws qapps get-q-app-session \
--session-id fill in from StartQAppSession response \
--instance-id qBusinessApplicationId \

//To provide follow up messages to an app that is waiting for additional input:

aws qapps update-q-app-session \
--session-id fill in from StartQAppSession response \
-- values '{"cardId":"fill in","value":"fill in"}'
--instance-id qBusinessApplicationId \
```

Document enrichment in Amazon Q Business

Important

This section assumes that you understand document attributes and metadata controls in Amazon Q Business.

Note

Before you configure document enrichment, you must create a Amazon Q Business retriever and index for your application.

The Amazon Q Business *document enrichment* feature helps you control both **what** documents and document attributes are ingested into your index and also **how** they're ingested. Using document enrichment, you can create, modify, or delete document attributes and document content when you ingest them into your Amazon Q Business index.

You can use document enrichment to provide more structure and context to the data that the large language model (LLM) powering Amazon Q Business uses to generate responses. This is done in the following ways:

- **Extracting metadata** – To make data easier for the LLM to understand, document enrichment extracts metadata like document title, type, and date and organizes these by mapping them to index fields.
- **Categorization** – Tagging documents with metadata categories helps the LLM recognize both content and context. This helps LLMs prioritize relevant sources when answering queries about specific categories.
- **Adding custom metadata** – By enriching documents with your own custom metadata, you can provide more relevant context for the LLM to work with.
- **Improved Relevance** – As a result of structured data and metadata enrichment, the LLM can better match user queries to the most relevant documents. This can lead to more accurate responses.

Document enrichment offers two kinds of methods that you can use for your solution:

- **Configure basic operations** – Use basic operations to add, update, or delete document attributes from your data. For example, you can scrub personally identifiable information (PII) by choosing to delete any document attributes related to PII.
- **Configure Lambda functions** – Use a preconfigured Lambda function to perform more customized, advanced document attribute manipulation logic to your data. For example, your enterprise data might be stored as scanned images. In that case, you can use a Lambda function to run Optical Character recognition (OCR) on the scanned documents to extract text from them. Then, each scanned document is treated as a text document during ingestion. Finally, during chat, Amazon Q Business will factor the textual data extracted from the scanned documents when it generates responses.

When you implement your solution, you can choose to use both document enrichment methods together. That is, you can use basic operations to do a first parse of your data and then use a Lambda function for more complex operations. For example, you could first use a basic function to remove all PII information from your documents using document attributes. Then, use a Lambda function to extract text from scanned documents.

You can use document enrichment on both the AWS Management Console and with Amazon Q Business API actions. If you use the console, you can only enrich documents connected to your application environment using an Amazon Q Business data source.

> **Note**
>
> Document enrichment is only supported in an Amazon Q Business application environment if you use an Amazon Q Business native retriever. If you use an Amazon Kendra retriever, we recommend that you configure document enrichment in Amazon Kendra.

Document enrichment limitations

When you use document enrichment, be aware of the following limitations that affect how you can process different types of content.

Multimedia content limitations

Document enrichment doesn't support the following multimedia file types:

- Audio files - You can't use document enrichment operations on audio content.
- Video files - You can't use document enrichment operations on video content.

Visual content in documents limitations

When you work with visual content in documents, the following limitations apply:

- If PostExtractionHook is configured, visual content in the document is ignored and not Indexed.

Connector-specific Document Enrichment behavior

When you enable visual content in documents, PreExtractionHookConfiguration operations for the following connectors are limited to metadata updates only:

- Web Crawler
- ServiceNow
- Confluence
- Salesforce
- SharePoint

Topics

- How Amazon Q Business document enrichment works
- Using basic operations for Amazon Q Business document enrichment
- Using Lambda functions for Amazon Q Business document enrichment

How Amazon Q Business document enrichment works

To understand and use document enrichments, familiarize yourself with the key Amazon Q Business concepts that this topic outlines.

Topics

- Document enrichment concepts
- Document enrichment process overview

Document enrichment concepts

Amazon Q Business extracts *document attributes* from any document that you ingest into an Amazon Q index. Document attributes or structural metadata can include document title, document type, and time and date created. You can map document attributes to fields in an Amazon Q Business index to better structure your data for retrieval and chat. For more information, see Document attributes and types and Filtering using document attributes.

> **Note**
>
> Although document attributes and index fields are distinct concepts, in practice they're used interchangeably because their values overlap and they structurally correspond to each other. That is, document attributes == document metadata == index fields.

Document enrichment process overview

The overall process of document enrichment is as follows:

- You configure document enrichment when you create or update your Amazon Q Business data source, or add or upload your documents directly into Amazon Q Business index. The exact process for configuration depends on the methods you choose:
  - If you use the API and want to configure document enrichment for a data source connector, you use the CreateDataSource and UpdateDataSource operations to provide your configuration details.
  - If you use the API and choose to directly upload documents into your index using the BatchPutDocument operation, you must configure document enrichment with each request.
  - If you use the console, can only configure document enrichment for a data source connected to your Amazon Q Business application environment. You select **Document enrichments** under **Enhancements** from the left navigation pane and configure enrichments. You can choose to use both configuration options or either one. You can also choose whether you want to apply your configuration to the original pre-extraction data or to the structured post-extraction data.
- After you configure and activate your document enrichment configuration, you can use inline configuration or basic logic to alter your data. For more information, see Using basic operations.
- If you chose to configure advanced data manipulation by using a Lambda function, Amazon Q Business applies the configured function (depending on what you've chosen) to either your

original pre-extraction data or your structured post-extraction data. For more information, see Using Lambda functions.

- Finally, your altered and enriched documents are ingested into your Amazon Q Business index.

If a configuration isn't valid during any point in this process, Amazon Q returns an error.

Using basic operations for Amazon Q Business document enrichment

With document enrichment, you can use basic operations to manipulate document attributes. For example, you can remove document attribute values, modify attribute values using conditions, or create document attributes.

> **Note**
>
> Amazon Q Business can't create a target document attribute field if it isn't already created as an index field.

Topics

- Basic operations using the Amazon Q Business API
- Basic operations using the Amazon Q Business console
- Use cases for basic operations
- Code examples of basic operations

Basic operations using the Amazon Q Business API

To apply basic logic, you specify your document attribute configuration using the DocumentAttributeTarget object when you use either the BatchPutDocument API operation or the CreateDataSource operation. Use the following parameters to create your configuration:

- `key` – The target field that you want to manipulate. For example, the key `Department` is a field or attribute that holds all the department names associated with the documents.
- `value` – The target value for your target attribute.
- `attributeValueOperator` – To delete an existing target value, set to `DELETE`. The default value for this parameter is `UPDATE`.

If a specific condition is met, you can also specify a value to use in the target field. Set the condition using the DocumentAttributeCondition object. For example, if the `_source_uri` field contains `financial` in its URI value, you can choose to pre-fill the target field `department` with the target value `finance` for the document.

For more information, see the following topics in the *Amazon Q Business API Reference*:

- BatchPutDocument
- CreateDataSource
- DocumentAttributeTarget
- DocumentAttributeCondition

Basic operations using the Amazon Q Business console

To apply basic logic using the console

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. From the left navigation menu, choose **Enhancements**, and then choose **Document enrichments**.
4. In **Document enrichments**, choose **Add document enrichment**.
5. In **Configure basic operations**, for **Document enrichment source**, choose a data source connected to your application environment.
6. To apply basic manipulations to your document fields and content, go to **Configure basic operations** .
7. Choose **Next** to save your configuration.

Use cases for basic operations

This section provides two examples of basic operations.

Example 1: Removing customer identification numbers associated with the documents

The following is an example of using a basic operation to remove all customer identification numbers in the document field called `customer_id`.

The following table shows the data before basic manipulation is applied.

_document_id	_document_body	customer_id
1	Example text	CID1234
2	Example text	CID1235
3	Example text	CID1236

The following table shows the data after basic manipulation is applied.

_document_id	_document_body	customer_id
1	Example text	
2	Example text	
3	Example text	

Example 2: Creating and pre-filling the Department field with department names associated with the documents using a condition

The following is an example of using basic logic to create a field called `Department` and pre-filling the field with the department names based on information from the `_source_uri` field. This example uses the condition that, if the `_source_uri` field contains `financial` in its URI value, then the target field `department` is pre-filled with the target value `finance` for the document.

The following table shows the data before basic manipulation is applied.

_document_id	document_body	_source_uri
1	Example text	financial/1
2	Example text	financial/2
3	Example text	financial/3

The following table shows the data after basic manipulation is applied.

_document_id	_document_body	_source_uri	department
1	Example text	financial/1	Finance
2	Example text	financial/2	Finance
3	Example text	financial/3	Finance

Code examples of basic operations

The following instructions give examples of configuring basic data manipulation to remove customer identification numbers associated with the documents.

Console

To configure basic data manipulation to remove customer identification numbers

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation pane, select **Document enrichments** and then select **Add document enrichment**.
3. On the **Configure basic operations** page, choose from the data source that you want to alter document fields and content in.
4. Select the document field name **Customer_ID** from the dropdown menu, and then select the target action **Delete**.
5. Select **Add basic operation**.

AWS CLI

To configure basic data manipulation to remove customer identification numbers

```
aws qbusiness create-data-source \
 --name data-source-name \
 --application-id application-id \
 --index-id index-id \
 --role-arn arn:aws:iam::account-id:role/role-name \
 --type S3 \
 --configuration '{"S3Configuration":{"BucketName":"S3-bucket-name"}}' \
```

```
 --document-enrichment-configuration '{"InlineDocumentEnrichmentConfiguration":
[{"Target":{"key":"Customer_ID", "attributeValueOperator": "DELETE"}}]}'
```

Python

To configure basic data manipulation to remove customer identification numbers

```
import boto3
from botocore.exceptions import ClientError
import pprint
import time

qbusiness = boto3.client("qbusiness")

print("Create a data source with customizations")

# Provide the name of the data source
name = "data-source-name"
# Provide the application environment ID for the data source
application_id = "application-id"
# Provide the index ID for the data source
index_id = "index-id"
# Provide the IAM role ARN required for data sources
role_arn = "arn:aws:iam::${account-id}:role/${role-name}"
# Provide the data source connection information
data_source_type = "S3"
S3_bucket_name = "S3-bucket-name"
# Configure the data source with Document Enrichment
configuration = {"S3Configuration":
        {
            "BucketName": S3_bucket_name
        }
    }
document_enrichment_configuration = {"InlineDocumentEnrichmentConfiguration":[
        {
            "Target":{"key":"Customer_ID",
                      "attributeValueOperator": "DELETE"}
        }]
    }

try:
    data_source_response = qbusiness.create_data_source(
        Name = name,
        ApplicationId = application_id,
```

```
        IndexId = index_id,
        RoleArn = role_arn,
        Type = data_source_type
        Configuration = configuration
        DocumentEnrichmentConfiguration = document_enrichment_configuration
    )

    pprint.pprint(data_source_response)

    data_source_id = data_source_response["Id"]

    print("Wait for Amazon Q to create the data source with your customizations.")

    while True:
        # Get the details of the data source, such as the status
        data_source_description = qbusiness.get_data_source(
            DataSourceId = data_source_id,
            ApplicationId = application_id,
            IndexId = index_id
        )
        status = data_source_description["Status"]
        print(" Creating data source. Status: "+status)
        time.sleep(60)
        if status != "CREATING":
            break

    print("Synchronize the data source.")

    sync_response = qbusiness.start_data_source_sync_job(
        DataSourceId = data_source_id,
        ApplicationId = application_id,
        IndexId = index_id
    )

    pprint.pprint(sync_response)

    print("Wait for the data source to sync with the index.")

    while True:

        jobs = qbusiness.list_data_source_sync_jobs(
            DataSourceId = data_source_id,
            ApplicationId = application_id,
            IndexId = index_id
```

```
        )

        # For this example, there should be one job
        status = jobs["History"][0]["Status"]

        print(" Syncing data source. Status: "+status)
        time.sleep(60)
        if status != "SYNCING":
            break

except  ClientError as e:
        print("%s" % e)

print("Program ends.")
```

Java

To configure basic data manipulation to remove customer identification numbers

```
package com.amazonaws.qbusiness;

import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.services.qbusiness.QBusinessClient;
import software.amazon.awssdk.services.qbusiness.model.AttributeValueOperator;
import software.amazon.awssdk.services.qbusiness.model.CreateDataSourceRequest;
import software.amazon.awssdk.services.qbusiness.model.CreateDataSourceResponse;
import software.amazon.awssdk.services.qbusiness.model.CreateIndexRequest;
import software.amazon.awssdk.services.qbusiness.model.CreateIndexResponse;
import software.amazon.awssdk.services.qbusiness.model.DataSourceConfiguration;
import software.amazon.awssdk.services.qbusiness.model.DataSourceStatus;
import software.amazon.awssdk.services.qbusiness.model.DataSourceSyncJob;
import software.amazon.awssdk.services.qbusiness.model.DataSourceSyncJobStatus;
import software.amazon.awssdk.services.qbusiness.model.DataSourceType;
import software.amazon.awssdk.services.qbusiness.model.GetDataSourceRequest;
import software.amazon.awssdk.services.qbusiness.model.GetDataSourceResponse;
import software.amazon.awssdk.services.qbusiness.model.IndexStatus;
import
 software.amazon.awssdk.services.qbusiness.model.ListDataSourceSyncJobsRequest;
import
 software.amazon.awssdk.services.qbusiness.model.ListDataSourceSyncJobsResponse;
import software.amazon.awssdk.services.qbusiness.model.DataSourceConfiguration;
import
 software.amazon.awssdk.services.qbusiness.model.StartDataSourceSyncJobRequest;
```

```
import
 software.amazon.awssdk.services.qbusiness.model.StartDataSourceSyncJobResponse;

public class CreateDataSourceWithCustomizationsExample {

    public static void main(String[] args) throws InterruptedException {
        System.out.println("Create a data source with customizations");

        String dataSourceName = "data-source-name";
        String applicationId = "application-id";
        String indexId = "index-id";
        String dataSourceRoleArn = "arn:aws:iam::account-id:role/role-name";
        String s3BucketName = "S3-bucket-name"

        QBusinessClient qbusiness = QBusinessClient.builder().build();

        CreateDataSourceRequest createDataSourceRequest = CreateDataSourceRequest
            .builder()
            .name(dataSourceName)
            .applicationId(applicationId)
            .indexId(indexId)
            .description(experienceDescription)
            .roleArn(experienceRoleArn)
            .type(DataSourceType.S3)
            .configuration(
                DataSourceConfiguration
                    .builder()
                    .s3Configuration(
                        S3DataSourceConfiguration
                            .builder()
                            .bucketName(s3BucketName)
                            .build().Q Business carries
                    ).build()
            )
            .documentEnrichmentConfiguration(
                DocumentEnrichmentConfiguration
                    .builder()
                    .inlineDocumentEnrichmentConfiguration(Arrays.asList(
                        InlineDocumentEnrichmentConfiguration
                            .builder()
                            .target(
                                DocumentAttributeTarget
                                    .builder()
                                    .key("Customer_ID")
```

```
.attributeValueOperator(AttributeValueOperator.DELETE)
                                    .build())
                            .build()
                    )).build();

        CreateDataSourceResponse createDataSourceResponse =
qbusiness.createDataSource(createDataSourceRequest);
        System.out.println(String.format("Response of creating data source: %s",
createDataSourceResponse));

        String dataSourceId = createDataSourceResponse.id();
        System.out.println(String.format("Waiting for Amazon Q to create the data
source %s", dataSourceId));
        GetDataSourceRequest getDataSourceRequest = GetDataSourceRequest
            .builder()
            .applicationId(applicationId).Q Business carries
            .indexId(indexId)
            .datasourceId(dataSourceId)
            .build();

        while (true) {
            GetDataSourceResponse getDataSourceResponse =
qbusiness.getDataSource(getDataSourceRequest);

            DataSourceStatus status = getDataSourceResponse.status();
            System.out.println(String.format("Creating data source. Status: %s",
status));
            TimeUnit.SECONDS.sleep(60);
            if (status != DataSourceStatus.CREATING) {
                break;
            }
        }

        System.out.println(String.format("Synchronize the data source %s",
dataSourceId));
        StartDataSourceSyncJobRequest startDataSourceSyncJobRequest =
StartDataSourceSyncJobRequest
            .builder()
            .applicationId(applicationId)
            .indexId(indexId)
            .datasourceId(dataSourceId)
            .build();
```

```
        StartDataSourceSyncJobResponse startDataSourceSyncJobResponse =
 qbusiness.startDataSourceSyncJob(startDataSourceSyncJobRequest);
        System.out.println(String.format("Waiting for the data source to sync
 with the application environment %s index %s for execution ID %s", applicationId,
 indexId, startDataSourceSyncJobResponse.executionId()));

        // For this example, there should be one job
        ListDataSourceSyncJobsRequest listDataSourceSyncJobsRequest =
 ListDataSourceSyncJobsRequest
            .builder()
            .applicationId(applicationId)
            .indexId(indexId)
            .datasourceId(dataSourceId)
            .build();

        while (true) {
            ListDataSourceSyncJobsResponse listDataSourceSyncJobsResponse =
 qbusiness.listDataSourceSyncJobs(listDataSourceSyncJobsRequest);
            DataSourceSyncJob job = listDataSourceSyncJobsResponse.history().get(0);
            System.out.println(String.format("Syncing data source. Status: %s",
 job.status()));

            TimeUnit.SECONDS.sleep(60);
            if (job.status() != DataSourceSyncJobStatus.SYNCING) {
                break;
            }

        }

        System.out.println("Data source creation with customizations is complete");
    }
}
```

Using Lambda functions for Amazon Q Business document enrichment

You can use Lambda functions to prepare your document attributes for advanced data manipulation. For example, you could use Optical Character Recognition (OCR), which interprets text from images and treats each image as a textual document. Or, you could retrieve the current date-time in a specific time zone and then insert the date-time where there's an empty value for a date field.

You can choose to apply a basic operation first and then use a Lambda function to manipulate your data, and the reverse.

Amazon Q Business requires an Amazon S3 bucket when using Lambda functions for custom document enrichment. This bucket serves as temporary storage during document processing. Amazon Q Business carries out the following steps when interacting with an Amazon S3 bucket:

1. Before invoking the Lambda function, Amazon Q Business uploads the document to your Amazon S3 bucket.
2. Your Lambda function code must get the document from the bucket and may then processes it.
3. Your Lambda code must put the processed document into the bucket for Amazon Q Business to retrieve.
4. You inform Amazon Q Business what updated document to retrieve using parameters in the return parameter.
5. Amazon Q Business retrieves the processed document and continues.

> **Note**
>
> Amazon Q Business can't create a target document attribute field if it isn't already created as an index field.

Topics

- Lambda functions using the Amazon Q Business API
- Lambda functions using the Amazon Q Business console
- IAM roles for Lambda functions
- Use cases for Lambda functions
- Code examples of Lambda functions
- Data contracts for Lambda functions

Lambda functions using the Amazon Q Business API

To apply a Lambda function, you specify your advanced data manipulation logic using the DocumentEnrichmentConfiguration object when you use either the BatchPutDocument API operation or the CreateDataSource operation.

Your Lambda functions must follow the mandatory request and response structures. For more information, see Data contracts for Lambda functions.

Use the following parameters to create your configuration:

- `InlineDocumentEnrichmentConfiguration` – Configuration information to alter document attributes during ingestion.
- `PostExtractionHookConfiguration` – Configuration information to invoke a Lambda function on structured documents with their metadata and text already extracted.
- `PreExtractionHookConfiguration` – Configuration information to invoke a Lambda function on raw documents before metadata and text has been extracted from them.
- `PreExtractionHookConfiguration` RoleArn – The Amazon Resource Name (ARN) of a role under `PreExtractionHookConfiguration` with permissions to run `PreExtractionHookConfiguration` and to access the Amazon S3 bucket when you use `PreExtractionHookConfiguration`.
- `PostExtractionHookConfiguration` RoleArn – The Amazon Resource Name (ARN) of a role under `PostExtractionHookConfiguration` with permissions to run `PreExtractionHookConfiguration` and to access the Amazon S3 bucket when you use `PostExtractionHookConfiguration`.

You can configure only one Lambda function for `PreExtractionHookConfiguration` and only one Lambda function for `PostExtractionHookConfiguration`. However, your Lambda function can invoke other functions that it requires.

You can configure both `PreExtractionHookConfiguration` and `PostExtractionHookConfiguration` or either one. Your Lambda function for `PreExtractionHookConfiguration` must not exceed a run time of 5 minutes. Your Lambda function for `PostExtractionHookConfiguration` must not exceed a run time of 1 minute.

You can configure Amazon Q Business to invoke a Lambda function only if a condition is met. For example, you can specify a condition that, if there are empty date-time values, then Amazon Q Business invokes a function that inserts the current date-time.

For more information, see the following topics in the *Amazon Q Business API Reference*:

- BatchPutDocument
- CreateDataSource

- DocumentEnrichmentConfiguration
- DocumentAttributeCondition

Lambda functions using the Amazon Q Business console

To configure a Lambda function using the console

1. Select your index, and then select **Document enrichments** from the navigation menu.
2. To configure Lambda functions, go to **Configure Lambda functions**.

IAM roles for Lambda functions

When you use the Lambda functions for CDE, you need an IAM role for the following:

- A role for `PreExtractionHookConfiguration` with permissions to run `PreExtractionHookConfiguration` and to access the Amazon S3 bucket when you use `PreExtractionHookConfiguration`.
- A role for `PostExtractionHookConfiguration` with permissions to run `PreExtractionHookConfiguration` and to access the Amazon S3 bucket when you use `PostExtractionHookConfiguration`.

> **Important**
>
> IAM roles for Custom Document Enrichmmnt (CDE) Lambda functions should belong to the same account as the account using BatchPutDocument API operation or the CreateDataSource operation to configure CDE.

Both AWS Identity and Access Management (IAM) roles must have the permissions to:

- Run `PreExtractionHookConfiguration` and/or `PostExtractionHookConfiguration`. To apply advanced alterations of your document metadata and content during the ingestion process, configure a Lambda function for `PreExtractionHookConfiguration` and/or `PostExtractionHookConfiguration`.

- (Optional) If you choose to activate Server Side Encryption for your Amazon S3 bucket, you must provide permissions to use the AWS KMS key to encrypt and decrypt the objects stored in your Amazon S3 bucket.

A role policy to allow Amazon Q Business to run `PreExtractionHookConfiguration` with encryption for your Amazon S3 bucket.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Effect": "Allow",
            "Sid": "S3GetObjectPermissions"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name"
            ],
            "Effect": "Allow",
            "Sid": "S3ListBucketPermissions"
        },
        {
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/key-id"
```

```
            ],
            "Effect": "Allow",
            "Sid": "KMSPermissions"
        },
        {
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": "arn:aws:lambda:us-east-1:111122223333:function:pre-
extraction-lambda-function",
            "Effect": "Allow",
            "Sid": "LambdaPermissions"
        }
    ]
}
```

An role policy to allow Amazon Q Business to run `PreExtractionHookConfiguration` without encryption.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Effect": "Allow",
            "Sid": "S3GetObjectPermissions"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::bucket-name"
            ],
            "Effect": "Allow",
            "Sid": "S3ListBucketPermissions"
        },
        {
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": "arn:aws:lambda:us-east-1:111122223333:function:pre-
extraction-lambda-function",
            "Effect": "Allow",
            "Sid": "LambdaPermissions"
        }
    ]
}
```

A role policy to allow Amazon Q Business to run `PostExtractionHookConfiguration` with Default (server-side encryption with S3-managed keys (SSE-S3) for your Amazon S3 bucket.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Effect": "Allow",
            "Sid": "S3GetObjectPermissions"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::bucket-name"
            ],
            "Effect": "Allow",
            "Sid": "S3ListBucketPermissions"
        },
        {
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow",
            "Sid": "KMSPermissions"
        },
        {
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": "arn:aws:lambda:us-east-1:111122223333:function:post-
extraction-lambda-function",
            "Effect": "Allow",
            "Sid": "LambdaPermissions"
        }
    ]
}
```

A role policy to allow Amazon Q Business to run `PostExtractionHookConfiguration` with encryption for your Amazon S3 bucket.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
```

```
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Effect": "Allow",
            "Sid": "S3GetObjectPermissions"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name"
            ],
            "Effect": "Allow",
            "Sid": "S3ListBucketPermissions"
        },
        {
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/key-id"
            ],
            "Effect": "Allow",
            "Sid": "KMSPermissions"
        },
        {
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": "arn:aws:lambda:us-east-1:111122223333:function:post-
extraction-lambda-function",
            "Effect": "Allow",
            "Sid": "LambdaPermissions"
        }
    ]
}
```

An role policy to allow Amazon Q Business to run `PostExtractionHookConfiguration` without encryption.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Effect": "Allow",
            "Sid": "S3GetObjectPermissions"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name"
            ],
            "Effect": "Allow",
            "Sid": "S3ListBucketPermissions"
        },
        {
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": "arn:aws:lambda:us-east-1:111122223333:function:post-
extraction-lambda-function",
            "Effect": "Allow",
            "Sid": "LambdaPermissions"
        }
    ]
}
```

We recommend that you include `aws:sourceAccount` and `aws:sourceArn` in the trust policy. Their inclusion limits permissions and securely checks if `aws:sourceAccount` and `aws:sourceArn` are the same values as provided in the IAM role policy for the `sts:AssumeRole` action. This approach prevents unauthorized entities from accessing your IAM roles and their permissions. For more information, see confused deputy problem in the *IAM User Guide*.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Sid": "QBusinessTrustPolicy",
            "Effect": "Allow",
            "Condition": {
                "StringLike": {
                    "aws:SourceArn": "arn:aws:qbusiness:your-
region:123456789012:application/<application-id>/index/<index-id>"
                },
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                }
            },
            "Principal": {
                "Service": [
                    "qbusiness.amazonaws.com"
                ]
            }
        }
    ]
}
```

Use cases for Lambda functions

This section outlines two examples of using Lambda functions.

Example 1: Extracting text from images to create textual documents

The following is an example of using a Lambda function to run OCR to interpret text from images and store this text in a field called `document_image_text`.

The following table shows data before advanced manipulation is applied.

_document_id	document_image
1	image_1.png
2	image_2.png
3	image_3.png

The following table shows data after advanced manipulation is applied.

_document_id	document_image	document_image_text
1	image_1.png	Mailed survey response
2	image_2.png	Mailed survey response
3	image_3.png	Mailed survey response

Example 2: Replacing empty values in the Last_Updated field with the current date-time

The following is an example of using a Lambda function to insert the current date-time for empty date values. This example uses the condition that, if a date field value is `null`, then the value is replaced with the current date-time.

The following table shows data before advanced manipulation is applied.

_document_id	_document_body	_last_updated_at
1	Example text	January 1, 2020
2	Example text	
3	Example text	July 1, 2020

The following table shows data after advanced manipulation is applied.

_document_id	_document_body	_last_updated_at
1	Example text	January 1, 2020
2	Example text	December 1, 2021
3	Example text	July 1, 2020

Code examples of Lambda functions

The following code is an example of configuring a Lambda function for advanced data manipulation on the raw, original data.

Console

To configure a Lambda function for advanced data manipulation on the raw, original data

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation menu, choose **Enhancements**, and then choose **Document enrichments**.
3. In **Document enrichments**, choose **Add document enrichment**.
4. In **Configure basic operations**, for **Document enrichment source**, choose a data source connected to your application environment.
5. (Optional) To apply basic manipulations to your document fields and content, go to **Configure basic operations** and choose **Next** to save your configuration.
6. On the **Configure Lambda functions** page, in the **Lambda for pre-extraction** section, select your Lambda function ARN and your Amazon S3 bucket using the dropdown menus.
7. To add your IAM access role, select the option to create a new role from the dropdown. This step creates the required Amazon Q Business permissions to create the document enrichment.
8. Select **Add basic operation**.

AWS CLI

To configure a Lambda function for advanced data manipulation on the raw, original data

```
aws qbusiness create-data-source \
```

```
 --display-name data-source-name \
 --application-id application-id \
 --index-id index-id \
 --role-arn arn:aws:iam::account-id:role/role-name \
 --configuration '{"connectionConfiguration":{"repositoryEndpointMetadata":
{"BucketName":"S3-bucket-name"}}, "type":"S3", "syncMode": "Sync-Mode-Type",
 "repositoryConfigurations":{"document":{"fieldMappings":
[{"dataSourceFieldName":"s3_document_id","indexFieldName":"s3_document_id","indexFieldType":
 \
 --document-enrichment-configuration '{"inlineConfigurations":[{"target":
{"key":"_file_type","value":{"stringValue":"file-type"}},
 "condition":{"key":"_file_type","operator":"operator-type","value":
{"stringValue":"file-type"}}}]}'
```

Python

To configure a Lambda function for advanced data manipulation on the raw, original data

```
import boto3
from botocore.exceptions import ClientError
import pprint
import time

qbusiness = boto3.client("qbusiness")

print("Create a data source with customizations")

# Provide the name of the data source
name = "data-source-name"
# Provide the application ID for the data source
application_id = "application-id"
# Provide the index ID for the data source
index_id = "index-id"
# Provide the IAM role ARN required for data sources
role_arn = "arn:aws:iam::${account-id}:role/${role-name}"
# Provide the data source connection information
data_source_type = "S3"
S3_bucket_name = "S3-bucket-name"
# Configure the data source with Document Enrichment
configuration = {"S3Configuration":
        {
            "BucketName": S3_bucket_name
        }
    }
```

```
document_enrichment_configuration = {"InlineDocumentEnrichmentConfiguration":[
        {
            "Target":{"key":"Customer_ID",
                      "attributeValueOperator": "DELETE"}
        }]
    }

try:
    data_source_response = qbusiness.create_data_source(
        Name = name,
        ApplicationId = application_id,
        IndexId = index_id,
        RoleArn = role_arn,
        Type = data_source_type
        Configuration = configuration
        DocumentEnrichmentConfiguration = document_enrichment_configuration
    )

    pprint.pprint(data_source_response)

    data_source_id = data_source_response["Id"]

    print("Wait for Amazon Q to create the data source with your customizations.")

    while True:
        # Get the details of the data source, such as the status
        data_source_description = qbusiness.get_data_source(
            DataSourceId = data_source_id,
            ApplicationId = application_id,
            IndexId = index_id
        )
        status = data_source_description["Status"]
        print(" Creating data source. Status: "+status)
        time.sleep(60)
        if status != "CREATING":
            break

    print("Synchronize the data source.")

    sync_response = qbusiness.start_data_source_sync_job(
        DataSourceId = data_source_id,
        ApplicationId = application_id,
        IndexId = index_id
    )
```

```
    pprint.pprint(sync_response)

    print("Wait for the data source to sync with the index.")

    while True:

        jobs = qbusiness.list_data_source_sync_jobs(
            DataSourceId = data_source_id,
            ApplicationId = application_id,
            IndexId = index_id
        )

        # For this example, there should be one job
        status = jobs["History"][0]["Status"]

        print(" Syncing data source. Status: "+status)
        time.sleep(60)
        if status != "SYNCING":
            break

except  ClientError as e:
        print("%s" % e)

print("Program ends.")
```

Java

To configure a Lambda function for advanced data manipulation on the raw, original data

```
package com.amazonaws.qbusiness;

import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.services.qbusiness.QBusinessClient;
import software.amazon.awssdk.services.qbusiness.model.AttributeValueOperator;
import software.amazon.awssdk.services.qbusiness.model.CreateDataSourceRequest;
import software.amazon.awssdk.services.qbusiness.model.CreateDataSourceResponse;
import software.amazon.awssdk.services.qbusiness.model.CreateIndexRequest;
import software.amazon.awssdk.services.qbusiness.model.CreateIndexResponse;
import software.amazon.awssdk.services.qbusiness.model.DataSourceConfiguration;
import software.amazon.awssdk.services.qbusiness.model.DataSourceStatus;
import software.amazon.awssdk.services.qbusiness.model.DataSourceSyncJob;
import software.amazon.awssdk.services.qbusiness.model.DataSourceSyncJobStatus;
import software.amazon.awssdk.services.qbusiness.model.DataSourceType;
```

```
import software.amazon.awssdk.services.qbusiness.model.GetDataSourceRequest;
import software.amazon.awssdk.services.qbusiness.model.GetDataSourceResponse;
import software.amazon.awssdk.services.qbusiness.model.IndexStatus;
import
 software.amazon.awssdk.services.qbusiness.model.ListDataSourceSyncJobsRequest;
import
 software.amazon.awssdk.services.qbusiness.model.ListDataSourceSyncJobsResponse;
import software.amazon.awssdk.services.qbusiness.model.DataSourceConfiguration;
import
 software.amazon.awssdk.services.qbusiness.model.StartDataSourceSyncJobRequest;
import
 software.amazon.awssdk.services.qbusiness.model.StartDataSourceSyncJobResponse;

public class CreateDataSourceWithCustomizationsExample {

    public static void main(String[] args) throws InterruptedException {
        System.out.println("Create a data source with customizations");

        String dataSourceName = "data-source-name";
        String applicationId = "application-id";
        String indexId = "index-id";
        String dataSourceRoleArn = "arn:aws:iam::account-id:role/role-name";
        String s3BucketName = "S3-bucket-name"

        QBusinessClient qbusiness = QBusinessClient.builder().build();

        CreateDataSourceRequest createDataSourceRequest = CreateDataSourceRequest
            .builder()
            .name(dataSourceName)
            .applicationId(applicationId)
            .indexId(indexId)
            .description(experienceDescription)
            .roleArn(experienceRoleArn)
            .type(DataSourceType.S3)
            .configuration(
                DataSourceConfiguration
                    .builder()
                    .s3Configuration(
                        S3DataSourceConfiguration
                            .builder()
                            .bucketName(s3BucketName)
                            .build()
                    ).build()
            )
```

```
            .documentEnrichmentConfiguration(
                DocumentEnrichmentConfiguration
                    .builder()
                    .inlineConfigurations(Arrays.asList(
                        InlineDocumentEnrichmentConfiguration
                            .builder()
                            .target(
                                DocumentAttributeTarget
                                    .builder()
                                    .key("Customer_ID")

.attributeValueOperator(AttributeValueOperator.DELETE)
                                    .build())
                            .build()
                    )).build();

       CreateDataSourceResponse createDataSourceResponse =
qbusiness.createDataSource(createDataSourceRequest);
       System.out.println(String.format("Response of creating data source: %s",
createDataSourceResponse));

       String dataSourceId = createDataSourceResponse.id();
       System.out.println(String.format("Waiting for Amazon Q to create the data
source %s", dataSourceId));
       GetDataSourceRequest getDataSourceRequest = GetDataSourceRequest
           .builder()
           .applicationId(applicationId)
           .indexId(indexId)
           .datasourceId(dataSourceId)
           .build();

       while (true) {
           GetDataSourceResponse getDataSourceResponse =
qbusiness.getDataSource(getDataSourceRequest);

           DataSourceStatus status = getDataSourceResponse.status();
           System.out.println(String.format("Creating data source. Status: %s",
status));
           TimeUnit.SECONDS.sleep(60);
           if (status != DataSourceStatus.CREATING) {
               break;
           }
       }
```

```
        System.out.println(String.format("Synchronize the data source %s",
 dataSourceId));
        StartDataSourceSyncJobRequest startDataSourceSyncJobRequest =
 StartDataSourceSyncJobRequest
            .builder()
            .applicationId(applicationId)
            .indexId(indexId)
            .datasourceId(dataSourceId)
            .build();
        StartDataSourceSyncJobResponse startDataSourceSyncJobResponse =
 qbusiness.startDataSourceSyncJob(startDataSourceSyncJobRequest);
        System.out.println(String.format("Waiting for the data source to sync
 with the application %s index %s for execution ID %s", applicationId, indexId,
 startDataSourceSyncJobResponse.executionId()));

        // For this example, there should be one job
        ListDataSourceSyncJobsRequest listDataSourceSyncJobsRequest =
 ListDataSourceSyncJobsRequest
            .builder()
            .applicationId(applicationId)
            .indexId(indexId)
            .datasourceId(dataSourceId)
            .build();

        while (true) {
            ListDataSourceSyncJobsResponse listDataSourceSyncJobsResponse =
 qbusiness.listDataSourceSyncJobs(listDataSourceSyncJobsRequest);
            DataSourceSyncJob job = listDataSourceSyncJobsResponse.history().get(0);
            System.out.println(String.format("Syncing data source. Status: %s",
 job.status()));

            TimeUnit.SECONDS.sleep(60);
            if (job.status() != DataSourceSyncJobStatus.SYNCING) {
                break;
            }

        }

        System.out.println("Data source creation with customizations is complete");
    }
}
```

Data contracts for Lambda functions

Lambda functions for advanced data manipulation interact with Amazon Q Business data contracts. The contracts are the mandatory request and response structures of your Lambda functions. If your Lambda functions don't follow these structures, then Amazon Q Business produces an error. Your Lambda function for `PreExtractionHookConfiguration` should use the following request structure:

```
{
    "version": <str>,
    "dataBlobStringEncodedInBase64": <str>, //In the case of a data blob
    "s3Bucket": <str>, //In the case of an S3 bucket
    "s3ObjectKey": <str>, //In the case of an S3 bucket
    "metadata": <Metadata>
}
```

The `metadata` structure, which includes the `DocumentAttribute` structure, is as follows:

```
{
    "attributes": [<DocumentAttribute<]
}

DocumentAttribute
{
    "name": <str>,
    "value": <DocumentAttributeValue>
}

DocumentAttributeValue
{
    "stringValue": <str>,
    "integerValue": <int>,
    "longValue": <long>,
    "stringListValue": list<str>,
    "dateValue": <str>
}
```

Your Lambda function for `PreExtractionHookConfiguration` must adhere to the following response structure:

```
{
```

```
    "version": <str>,
    "dataBlobStringEncodedInBase64": <str>, //In the case of a data blob
    "s3ObjectKey": <str>, //In the case of an S3 bucket
    "metadataUpdates": [<DocumentAttribute>]
}
```

Your Lambda function for `PostExtractionHookConfiguration` should expect the following request structure:

```
{
    "version": <str>,
    "s3Bucket": <str>,
    "s3ObjectKey": <str>,
    "metadata": <Metadata>
}
```

Your Lambda function for `PostExtractionHookConfiguration` must adhere to the following response structure:

```
PostExtractionHookConfiguration Lambda Response
{
    "version": <str>,
    "s3ObjectKey": <str>,
    "metadataUpdates": [<DocumentAttribute>]
}
```

Amazon Q Business uploads your structured document to the specified Amazon S3 bucket. The structured document follows this format:

```
QBusiness document

{
   "textContent": <TextContent>
}

TextContent
{
  "documentBodyText": <str>
}
```

Examples of Lambda functions that adhere to data contracts

This section provides examples of how to structure your Lambda functions that adhere to Amazon Q Business data contracts.

Example 1: A Lambda function that applies advanced manipulation to raw documents

The following Python code is an example of a Lambda function that applies advanced manipulation of the metadata fields `_authors`, `_document_title`, and the body content on the raw or original documents.

The following code example shows the case of the body content residing in an Amazon S3 bucket

```
import json
import boto3

s3 = boto3.client("s3")

# Lambda function for advanced data manipulation
def lambda_handler(event, context):
    # Get the value of "S3Bucket" key name or item from the given event input
    s3_bucket = event.get("s3Bucket")
    # Get the value of "S3ObjectKey" key name or item from the given event input
    s3_object_key = event.get("s3ObjectKey")

    content_object_before_DE = s3.get_object(Bucket = s3_bucket, Key = s3_object_key)
    content_before_DE = content_object_before_DE["Body"].read().decode("utf-8");
    content_after_DE = "DEInvolved " + content_before_DE

    # Get the value of "metadata" key name or item from the given event input
    metadata = event.get("metadata")
    # Get the document "attributes" from the metadata
    document_attributes = metadata.get("attributes")

    s3.put_object(Bucket = s3_bucket, Key = "dummy_updated_qbusiness_document",
 Body=json.dumps(content_after_DE))
    return {
        "version": "v0",
        "s3ObjectKey": "dummy_updated_qbusiness_document",
        "metadataUpdates": [
            {"name":"_document_title", "value":
{"stringValue":"title_from_pre_extraction_lambda"}},
            {"name":"_authors", "value":{"stringListValue":["author1", "author2"]}}
        ]
```

```
    }
```

Example 2: A Lambda function that applies advanced manipulation to structured or parsed documents

The following Python code is an example of a Lambda function that applies advanced manipulation of the metadata fields `_authors`, `_document_title`, and the body content on the structured or parsed documents.

```
import json
import boto3
import time

s3 = boto3.client("s3")

# Lambda function for advanced data manipulation
def lambda_handler(event, context):

    # Get the value of "S3Bucket" key name or item from the given event input
    s3_bucket = event.get("s3Bucket")
    # Get the value of "S3ObjectKey" key name or item from the given event input
    s3_key = event.get("s3ObjectKey")
    # Get the value of "metadata" key name or item from the given event input
    metadata = event.get("metadata")
    # Get the document "attributes" from the metadata
    document_attributes = metadata.get("attributes")

    qbusiness_document_object = s3.get_object(Bucket = s3_bucket, Key = s3_key)
    qbusiness_document_string =
 qbusiness_document_object['Body'].read().decode('utf-8')
    qbusiness_document = json.loads(qbusiness_document_string)
    qbusiness_document["textContent"]["documentBodyText"] = "Changing document body to
 a short sentence."

    s3.put_object(Bucket = s3_bucket, Key = "dummy_updated_qbusiness_document",
 Body=json.dumps(qbusiness_document))

    return {
        "version" : "v0",
        "s3ObjectKey": "dummy_updated_qbusiness_document",
        "metadataUpdates": [
            {"name": "_document_title", "value":{"stringValue":
 "title_from_post_extraction_lambda"}},
```

```
            {"name": "_authors", "value":{"stringListValue":["author1", "author2"]}}
        ]
    }
```

Example 3: Body content residing in a data blob

```
import json
import boto3
import base64

# Lambda function for advanced data manipulation
def lambda_handler(event, context):

    # Get the value of "dataBlobStringEncodedInBase64" key name or item from the given
 event input
    data_blob_string_encoded_in_base64 = event.get("dataBlobStringEncodedInBase64")
    # Decode the data blob string in UTF-8
    data_blob_string =
 base64.b64decode(data_blob_string_encoded_in_base64).decode("utf-8")
    # Get the value of "metadata" key name or item from the given event input
    metadata = event.get("metadata")
    # Get the document "attributes" from the metadata
    document_attributes = metadata.get("attributes")

    new_data_blob = "This should be the modified data in the document by pre processing
 lambda ".encode("utf-8")
    return {
        "version": "v0",
        "dataBlobStringEncodedInBase64":
 base64.b64encode(new_data_blob).decode("utf-8"),
        "metadataUpdates": [
            {"name":"_document_title", "value":
{"stringValue":"title_from_pre_extraction_lambda"}},
            {"name":"_authors", "value":{"stringListValue":["author1", "author2"]}}
        ]
    }
```

Extracting semantic meaning from embedded visual content with Amazon Q Business

When Amazon Q Business processes your input files from a data source, it uses advanced image understanding capabilities to extract semantic information and insights from images and other visuals. For example, it can extract insights from bar charts, technical illustrations, or hierarchical organizational structures.

By extracting semantic meaning from embedded images, Amazon Q Business makes the visual information in your data sources queryable. This makes relevant information easier to find, even if it's conveyed in embedded diagrams or charts. This data provides additional context and nuance to the information in your data sources and builds a more complete knowledge base from your enterprise data.

You can enable content extraction when you add or update a data connector, or when you import a file directly. You can enable it by using the Amazon Q Business console or by using API operations. Processing documents that contain images and visuals takes more time than processing text-only documents.

When you enable content extraction for a connector, we recommend that you use incremental sync mode. If you enable full-sync for your connector, or if you import the same files individually, Amazon Q Business processes the file and corresponding images again. For more information about sync modes in Amazon Q Business, see Sync mode.

Extracting semantic meaning from embedded images and visuals incurs additional costs. For more information, see Amazon Q Business pricing.

When Amazon Q Business processes your input files from a data source, it uses advanced image understanding capabilities to extract semantic information and insights from images and other visuals. For example, it can extract insights from bar charts, technical illustrations, or hierarchical organizational structures. This capability now extends to images embedded in web pages, in addition to images in documents like PDFs and presentations.

Note

For data sources using web-crawler as the connector, only data sources created after 06/13/2025 will process images both in web-pages and attachments/linked-documents. Data sources created before 06/13/2025, will continue to process images only in

attachments/linked-documents (pdf, ppt, word). Please reach out to AWS support for enabling for existing datasources.

Topics

- End user experience
- Guidelines and requirements
- Extracting content from visuals with data connectors
- Extracting semantic meaning from audio and video content
- Extracting content from visuals in a file
- Downloading images to add to responses (API operations)

End user experience

After Amazon Q Business extracts semantic meaning from images and visuals, your end users can ask questions and get answers related to the images. When an end user asks a question, Amazon Q Business retrieves relevant answers from the text and the images. Answers include the images and links for the documents that contain them.

For example, your user might ask, "Can you walk me through the process of enrolling in a health plan on the employee benefits site?" Amazon Q Business would then analyze the company's internal knowledge base, including detailed guides, process documentation, and screen shots showing the step-by-step enrollment process. It would synthesize this information into a clear, easy-to-follow response that outlined each stage of the enrollment journey.

Guidelines and requirements

The following are guidelines and requirements for extracting content from images:

- Documents can have up to 3,000 pages.
- The IAM service role that grants Amazon Q Business permission to access your resources must have `qbusiness:GetMedia` permissions. For a policy example, see IAM role for an Amazon Q Business web experience using IAM Identity Center
- Image extraction is supported for the following image sources: PDF, PPT, Microsoft Word docs, Webpages (for Webcrawler), Google Slides and Google Docs (for Google Drive)

- You can use the following connectors:
  - Amazon S3
  - Google Drive - Supports embedded images for Google Slides and Google Docs
  - Confluence (Cloud)
  - Confluence (Server/Data Center)
  - SharePoint (Online)
  - SharePoint Server 2019
  - SharePoint Server 2016
  - Gmail
  - Microsoft Exchange
  - OneDrive
  - Amazon WorkDocs
  - Smartsheet
  - Jira
  - Slack
  - ServiceNow
  - Salesforce
  - Web Crawler - Supports embedded images
  - Microsoft Teams

Extracting content from visuals with data connectors

You can enable content extraction when you add or update a data connector with the Amazon Q Business console or API operations. Processing images and visuals takes more time than processing text-only for the documents.

Console

When you add or update a data connector, in the **Multi-media content configuration** section of **Sync scope**, choose **Visual content in documents**. For more information, see the console procedure for your data connector. For example, for a console procedure for Amazon S3, see Connecting Amazon Q Business to Amazon S3 using the console.

APIs

To enable content extraction from images when you use the CreateDataSource or UpdateDataSource API operations, for `mediaExtractionConfiguration` set `imageExtractionStatus` to ENABLED. The following example shows how to enable content extraction when you create a data source. After you turn on content extraction, you can view media extraction configuration for the data source with the GetDataSource API operation.

```
aws qbusiness create-data-source \
--application-id app-12345abcde \
--index-id index-67890fghij\
--display-name My New S3 Source \
--configuration '{
    "S3Configuration": {
      "BucketName": "my-s3-bucket",
      "DocumentsMetadataConfiguration": {
        "S3Prefix": "documents/"
      }
    }
}' \
--media-extraction-configuration '{
    "imageExtractionConfiguration": {
      "imageExtractionStatus": "ENABLED"
    }
}' \
--description Description of data source connector \
--role-arn arn:aws:iam::123456789012:role/AmazonQServiceRole
```

Extracting semantic meaning from audio and video content

Amazon Q Business extracts semantic information from audio and video files, making data sources queryable and enhancing information retrieval.

Capabilities

- Processes up to 10 GB of video and 2 GB of audio
- Builds a comprehensive knowledge base

Enabling Content Extraction

- Use the Amazon Q Business console or API

- Available when adding connectors or importing files

Audio and video extraction

The System extracts the following from audio and video files:

- Transcribed text from audio voice content
- Time-stamped indexing of content
- Summary and theme detection

> **Important**
>
> Processing multimedia content takes longer than text-only documents. Incremental sync mode is recommended for multimedia processing.

Query audio and video content using natural language, and explore deeper with follow-up questions.

Processing Considerations

- Audio and video files take longer to process than text-only files
- Amazon Q Business doesn't charge for re-synchronizations (re-syncs) when content remains unchanged.

Additional Information

- For sync modes, see Sync mode
- For pricing details, see Amazon Q Business pricing

Guidelines and requirements

The following guidelines and best practices apply to content extraction from audio and video. Supported formats:

- Audio files - MP3, WAV, M4A, FLAC, OGG

- Video files - MP4, MOV, M4V

File limitations:

- Audio and video maximum duration: 4 hours
- English-language content only

The following connectors use incremental sync mode for connectors processing multimedia content, and can consider additional costs for multimedia processing:

- Amazon S3
- Google Drive

Ingest Audio/Video documents using the console

1. Login to your personal AWS account
2. Create a new application or use an existing application

Ingest Audio/Video files using direct upload

Open the application, whether it is a newly created application or an application you have used previously:

1. Click **Add data source**
2. Select the **Upload Files** option
3. Upload a supported Audio/Video file
4. In the **File Indexing Configuration**, select the audio/video files option based on the files you uploaded
5. Click the upload button on the bottom right corner
6. Monitor the uploaded file source under the data source tab. The status will update in sequence: "Received" => "Processing" => "Indexed/Updated"
7. Once the status is Indexed/Updated, it means your file is indexed successfully

> **Note**
>
> For file uploads, the Audio/Video size limit is consistent with the general file size limit of 50 MB.

Ingest Audio/Video documents using data source

Open the application, whether it is a newly created application or an application you have used previously:

1. Click **Add data source**
2. Select any supported data source
3. Fill in the following information:
    a. Enter the data source name
    b. For the IAM role, select from the dropdown menu **Create new service role**
    c. Enter the S3 bucket containing the Audio/Video files in the **Data Source Location** field under **Sync scope**
    d. Set **Sync Mode** and **Sync Run** as per your requirement
    e. Click on **Add data source** on the bottom right corner
4. Navigate to the **Data sources** pag and select the data source created and click **Sync now**
5. Click on the data source created, wait for the sync to complete and verify no documents from the Sync history tab **Failed to be indexed**

Extracting content from visuals in a file

You can enable content extraction from a file with the Amazon Q Business console or API operations. Processing images and visuals takes more time than processing text-only for the documents.

Console

When you upload documents directly to an Amazon Q Business application environment, in the **Multi-media content configuration** section of **Select files**, choose the **Visual content in documents** option. For step by step instructions, see Uploading files.

APIs

To enable content extraction from a file when you use the BatchPutDocument API operation, in the `ImageExtractionConfiguration` you set the `imageExtractionStatus` to `ENABLED`.

```
aws qbusiness batch-put-document \
--application-id app-12345abcde \
--index-id index-67890fghij \
--role-arn arn:aws:iam::123456789012:role/ServiceRoleName \
--documents '[{
    "Id": "doc1",
    "MediaExtractionConfiguration": {
        "ImageExtractionConfiguration": {
            "ImageExtractionStatus": "ENABLED"
        }
    }
}]'
--data-source-sync-id sync-12345
```

Downloading images to add to responses (API operations)

If you have implemented your own application with the Amazon Q Business Chat and ChatSync APIs, you can use the GetMedia API operation to download the images to add to chat responses. You can find the `mediaId` using the Chat, ChatSync and ListMessages API operations. The `mediaId` is listed in the `textMessageSegments` as part of the source attribution.

> **Note**
>
> The `mediaBytes` field in the GetMedia API response contains binary image data that may not require base64 decoding, depending on your implementation.

```
aws qbusiness get-media \
--application-id app-12345abcde \
--conversation-id conv-67890fghij \
--media-id media-12345abcde \
--message-id msg-67890fghij
```

Tuning the query results based on document attribute relevancy

Important

This section assumes that you understand document attributes and metadata controls in Amazon Q Business.

Note

If you are already using metadata boosting, please contact AWS Support to migrate to the new version.
Relevancy tuning in Amazon Q Business is only available if you use an Amazon Q native retriever. If you use an Amazon Kendra retriever, you must configure boosting for document attributes in Amazon Kendra.

Relevance tuning or boosting is the ability for the admins to provide their preference based on document attributes that can guide the retrieval and response generation in Amazon Q Business. Choosing to boost document attributes doesn't by itself cause Amazon Q Business to include or exclude a document in the chat response. A boosted document attribute is only one of the factors that Amazon Q Business uses to determine the relevance of a document. You can provide preferences on recency of the documents or the data sources where the documents are stored using the metadata fields.

For more information, see Understanding boosting in Amazon Q Business

Topics

- Recency
- Sources
- Rank order
- Setting relevancy preferences

Recency

Recency is the preference when the documented was created or last updated. To tune for the results for recency, enable this preference. In **Recency type**, choose either the `_created_at` or `_last_updated_at` document attribute to indicate which metadata field to use to guide Amazon Q Business. After choosing a document attribute, set the time period in **Boosting duration** over which the boost applies to the `DATE` type document attribute. You can pick either the last three, six, nine, or 12 months to apply the boost.

For example, if you set boosting duration to the last three months for the `_created_at` reserved attribute, documents created within the last three months will be get a higher preference than documents created more than three months ago.

Generally, all documents inside the boosting duration will be given more importance over documents outside the boosting duration. Within the boosting duration, documents with more recent dates will be given more importance over documents with less recent dates. Outside the boosting duration, the documents will not get be any additional preference or boost.

Sources

Sources is the preference where the document is stored. This preference allows you to boost chat responses based on `_data_source_id` document attribute that helps you rank sources that are more authoritative than other sources in your application environment. You can select up to five data sources.

For example, you have a two data sources—Sharepoint and an S3 bucket. If you want Amazon Q Business to respond based on documents in S3 (if available) first and then look at documents stored in Sharepoint, rank S3 higher than Sharepoint.

If you enable both preferences, you can also set the rank order of the **Recency** and **Sources** preferences. For example, if where the document is stored is more important than when the document was created or updated, drag **Source** to have a higher priority than **Recency**.

Rank order

If you enable both preferences, you can also set the rank order of the **Recency** and **Sources** preferences. For example, if where the document is stored is more important than when the document was created or updated, drag **Source** to have a higher priority than **Recency**.

Setting relevancy preferences

The following tabs provide a procedure to tune the query responses based on document attributes using the console and code examples for the AWS CLI.

Console

To tune the relevancy based on recency or data source

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. From the left navigation menu under **Enhancements**, choose **Relevance tuning**.
4. Enable the attributes to tune the query responses.
5. Drag the attribute to the order you want to prioritize the attributes.
6. To prioritize responses from more recent documents, in **Recency**, set the **Recency Type** and **Boosting duration**. In **Recency Type**, choose the metadata field you want to use. For **Boosting duration**, choose the time periods to prioritize when searching through data sources. Documents that were created or updated outside of the specified time periods will not have additional boosting or priority.
7. To prioritize based on data sources, in **Sources**, choose a data source, and choose **Add a source**. You can choose up to five data sources to search for documents. Rank the data source based to define the priority to be used for responses.

AWS CLI

Update your Amazon Q Business index to apply relevancy tuning

This example shows how to increase the relevancy based on the `_last_update_at` metadata field. In this example, replace each *`user input placeholder`* with your own information:

```
aws qbusiness --region region update-retriever \
  --application-id application_id \
  --retriever-id retriever_id \
  --configuration '{
    "nativeIndexConfiguration": {
        "indexId": "index_id",
```

```
        "boostingOverride": {
          "_last_updated_at"|"_created_at": {
            "dateConfiguration": {
              "boostingLevel": "ONE"|"TWO",
              "boostingDurationInSeconds": long;
            }
          },
          "_data_source_id": {
            "stringConfiguration": {
              "boostingLevel": "ONE"|"TWO",
              "attributeValueBoosting": {
                "data_source_id_1": "ONE"|"TWO"|"THREE"|"FOUR"|"FIVE",
                "data_source_id_1": "ONE"|"TWO"|"THREE"|"FOUR"|"FIVE",
                ...
              }
            }
          }
        }
    }
  }'
```

This example shows an example input. Replace each *user input placeholder* with your own information:

```
aws qbusiness --region us-west-2 update-retriever \
  --endpoint-url https://endpoint-url \
  --application-id application_id
  --retriever-id retriever_id \
  --configuration '{
    "nativeIndexConfiguration": {
        "indexId": "index_id",
        "boostingOverride": {
          "_last_updated_at": {
            "dateConfiguration": {
              "boostingLevel": "ONE",
              "boostingDurationInSeconds": 100
            }
          },
          "_data_source_id": {
            "stringConfiguration": {
              "boostingLevel": "TWO",
```

```
            "attributeValueBoosting": {
              "data_source_id_1": "ONE",
              "data_source_id_1": "TWO",
              "data_source_id_1": "THREE",
              "data_source_id_1": "FOUR",
              "data_source_id_1": "FIVE"
            }
          }
        }
      }
    }
  }'
```

Boosting chat responses using metadata boosting

> **Note**
>
> Relevance tuning has replaced metadata boosting. For more information, see Tuning the query results based on document attribute relevancy.

> **Important**
>
> This section assumes that you understand document attributes and metadata controls in Amazon Q Business.

> **Note**
>
> Before you configure relevance tuning, you must create a Amazon Q Business retriever and index for your application.

If you choose to use an Amazon Q Business native retriever, you can assign weights to document attributes after mapping them to Amazon Q Business index fields using the Amazon Q Business *metadata boosting* feature. Then, you can use these assigned weights to fine-tune the underlying

ranking of RAG retrieved passages within your Amazon Q application environment to optimize the relevance of chat responses. In Amazon Q, boosting means to raise a document in chat results using these weights.

Important

Boosting document attributes using *metadata boosting* is an admin-only feature.

Boosting chat responses based on document attributes helps you rank sources that are more authoritative higher than other sources in your application environment. You can assign a higher value to more recent content, specific file types, or specific data sources.

Amazon Q Business automatically boosts specific document attributes, like document title, when retrieving information from your index to generate end user chat responses. You can use the boosting feature to customize and control boosting, and also override any pre-existing boosts applied by Amazon Q Business.

When you use this feature, a Retrieval Augmented Generation (RAG)-generated result is given a boost during retrieval when the query includes terms that match that field or attribute. You specify how much of a boost the document receives when there is a match. When Amazon Q Business generates responses, it prioritizes the sources that are assigned higher rankings.

Choosing to boost document attributes doesn't by itself cause Amazon Q Business to include or exclude a document in the chat response. A boosted document attribute is only one of the factors that Amazon Q Business uses to determine the relevance of a document.

Note

Boosting in Amazon Q Business is only available if you use an Amazon Q native retriever. If you use an Amazon Kendra retriever, you must configure boosting for document attributes in Amazon Kendra. Amazon Q Business supports any boosting that's already configured in your Amazon Kendra index.

Topics

- Understanding boosting in Amazon Q Business
- Amazon Q Business boosting types

- Configuring document attributes for boosting in Amazon Q Business
- Enabling document attributes for search in Amazon Q Business

Understanding boosting in Amazon Q Business

> **Note**
>
> Relevance tuning has replaced metadata boosting. For more information, see Tuning the query results based on document attribute relevancy.

To improve retrieved results and customize the end user chat experience, Amazon Q enables you to map attributes to fields in your Amazon Q Business index.

Amazon Q Business offers two kinds of attributes:

- **Reserved or default** – Reserved attributes are based on document attributes that commonly occur in most data. You can use reserved attributes to map commonly occurring document attributes in your data to Amazon Q Business index fields.
- **Custom** – You can create custom attributes to map document attributes that are unique to your data to Amazon Q Business index fields.

Document attributes can be mapped to index fields using either the Amazon Q console or the API:

- **Use the API** – Before you use the API, you must first create an index. Next, create index fields. Then, to ingest documents into your Amazon Q Business index, use the CreateDataSource or BatchPutDocument API operations.
- **Use the console** – You can choose to map document attributes directly to your index or from your data sources when you connect your data source to Amazon Q Business.

  You can create and map document attributes to index fields using the *Metadata* function on the console.

  When you use data sources the your document attributes are added using data sources, Amazon Q Business automatically maps specific data source document fields to Amazon Q Business index fields. You can choose to add custom fields during the data source configuration process as well.

Document attributes—both reserved and custom—can only be of the following data types: `DATE`, `NUMBER`, `STRING`, and `STRING_LIST`. To use `STRING` and `STRING_LIST` type document attributes for boosting on the console and the API, they must be enabled for search. To enable these attributes using API, use the DocumentAttributeConfiguration object of the UpdateIndex API operation.

To customize and control boosting for document attributes, use the `boostingOverride` parameter of the NativeIndexConfiguration object of the UpdateRetriever API operation.

To enable these attributes using the console, follow the steps in Mapping document attributes directly to index fields.

> **Note**
>
> If you don't enable search on these attributes, you can't boost attributes of these data types on either the Amazon Q Business console or the API.

For more information about Amazon Q Business document attributes and how to map them, see Document attributes and types.

Amazon Q Business boosting types

> **Note**
>
> Relevance tuning has replaced metadata boosting. For more information, see Tuning the query results based on document attribute relevancy.

Amazon Q Business offers two types of boosting: document attribute boosting and document attribute value boosting. This section outlines how these types of boosting work.

> **Note**
>
> To use the `STRING` and `STRING_LIST` type document attributes for boosting on the console and the API, they must be enabled for search using the DocumentAttributeConfiguration object of the UpdateIndex API operation. If you don't

enable search on these attributes, you can't boost attributes of these data types on either the Amazon Q Business console or the API.

Types of boosting

- Boosting document attribute importance
- Boosting document attribute value

Boosting document attribute importance

> **Note**
>
> Relevance tuning has replaced metadata boosting. For more information, see Tuning the query results based on document attribute relevancy.

You can boost document attributes to control the relative importance, or boosting level, of the field for end user queries. You can boost importance for all document attribute data types that are supported by Amazon Q—`DATE`, `NUMBER`, `STRING`, and `STRING_LIST`.

> **Note**
>
> Amazon Q Business automatically boosts the document title attribute to **Low**. You can change this value when you customize boosting.

If you choose to boost document attributes, you can also customize boosting in the following ways:

- **Boost duration** – Specifies the time period over which a boost applies to a `DATE` type document attribute. For example, if you set boosting duration to 604,800 seconds (1 week) for the `_created_at` reserved attribute, documents created within the last week will be boosted.

  Generally, all documents inside the boosting duration will be given more importance over documents outside the boosting duration. Within the boosting duration, documents with more recent dates will be given more importance over documents with less recent dates.

Outside the boosting duration, the documents with more recent dates will continue to be given more importance over documents with less recent dates. However, the overall effect of the date boosting will taper to zero as the dates move further away from the boosting duration.

> **Note**
>
> Boosting duration is based on the most recent date in all documents in the index.

- **Boost order** – Determines whether a `NUMBER` type document attribute is boosted in prioritizing higher values or prioritizing lower values.

  For example, if your documents contain attributes for view count, you can choose to prioritize chat responses with higher view count values by boosting larger values over smaller values. Or, suppose your documents contain attributes that denote priority—for example, a task tracker that assigns priority 1 to the most important task. In that case, you can choose to boost documents using smaller values.

Boosting document attribute value

> **Note**
>
> Relevance tuning has replaced metadata boosting. For more information, see Tuning the query results based on document attribute relevancy.

To customize boosting levels, you can boost document attribute values for only `STRING` type document attributes.

For example, suppose that you're applying an importance boost to a `STRING` attribute called `department`. The `department` attribute has values like `HR` and `Legal`. You can assign the values `HR, VERY_HIGH` and `Legal, HIGH` to customize the importance that Amazon Q gives to these attribute values when they match a chat request.

Configuring document attributes for boosting in Amazon Q Business

> **Note**
>
> Relevance tuning has replaced metadata boosting. For more information, see Tuning the query results based on document attribute relevancy.

To boost specific documents for end user queries using document attributes, you can use the AWS Management Console or the DocumentAttributeBoostingConfiguration parameter of the UpdateRetriever API operation.

> **Note**
>
> For `STRING` and `STRING_LIST` type document attributes to be used for boosting on the console and the API, they must be enabled for search using the DocumentAttributeConfiguration object of the UpdateIndex API operation. If you don't enable search on these attributes, you can't boost attributes of these data types on either the console or the API.

The following tabs provide a procedure to boost document attributes using the console and code examples for the AWS CLI.

Console

To boost document attributes

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. In **Applications**, select the name of your application environment from the list of applications.
3. From the left navigation menu, choose **Metadata boosting**.
4. In **Metadata boosting**, choose the document attribute type that you want to boost.

   > **Note**
   >
   > You can boost attributes using the following values: **None**, **Low**, **Medium**, **High**, and **Very high**.

Choose from the following options:

a. **Popular** – Amazon Q displays the following popularly boosted document attributes for you to choose from:

   i. **Document title** – Use to boost the title of a document. You can also use **Advanced settings** to boost specific document titles. By default, the document title attribute is enabled for search with a value of `Low`. You can change this value when you customize boosting.

   ii. **Last updated** – Use to boost content by its last updated date. You can also use **Advanced settings** to configure **Boosting duration**, or how long your boost should apply.

   iii. **File type** – Use to boost content by file type.

   iv. **Data sources** – Use to boost the content data source type.

   v. To save your configuration, choose **Save**.

b. **Text** – Use to boost `STRING` and `STRING_LIST` type reserved or custom document attributes that you have enabled for search. Then, choose **Save**.

c. **Date** – Use to boost content using `DATE` type reserved or custom document attributes. For example, use the **Created at** document attribute to boost content based on recency. You can also use **Advanced settings** to configure **Boosting duration**, or how long your boost should apply. Then, choose **Save**.

d. **Numeric** – Use to boost content using `NUMERIC` type reserved or custom attributes. For example, use the **View count** document attribute to boost content based on view count. Based on your boosting needs, choose either **Prioritize higher values** or **Prioritize lower values**. Then, choose **Save**.

e. Once done, you can select **View web experience** to check boosting. Your configured web experience will open in a new window.

AWS CLI

Update your Amazon Q Business index to apply boosting

This example shows how to apply `VERY_HIGH` boosting for the `STRING` type document attribute `_document_title`.

```
aws qbusiness update-retriever \
--application-id APPLICATION-ID --retriever-id RETRIEVER-ID \
--configuration '{
        "nativeIndexConfiguration": {
            "indexId": "INDEX-ID",
            "boostingOverride": {
                "_document_title": {
                    "stringConfiguration": {
                        "boostingLevel": "VERY_HIGH"
                    }
                }
            }
        }
}'
```

This example shows how to apply boosting for the `STRING` type attribute `_category`, the `DATE` type attribute `_created_at`, the `NUMBER` type attribute `_view_count`, and the `STRING_LIST` type attribute `_authors`.

```
aws qbusiness update-retriever \
--application-id APPLICATION-ID --retriever-id RETRIEVER-ID \
--configuration '{
        "nativeIndexConfiguration": {
            "indexId": "INDEX-ID",
            "boostingOverride": {
                "_category": {
                    "stringConfiguration": {
                        "boostingLevel": "LOW",
                        "attributeValueBoosting": {
                            "HR": "MEDIUM"
                        }
                    }
                },
                "_created_at": {
                    "dateConfiguration": {
                        "boostingLevel": "LOW",
                        "boostingDurationInSeconds": 2592000
                    }
                },
                "_view_count": {
```

```
                    "numberConfiguration": {
                        "boostingLevel": "LOW",
                        "boostingType": "PRIORITIZE_SMALLER_VALUES"
                    }
                },
                "_authors": {
                    "stringListConfiguration": {
                        "boostingLevel": "HIGH"
                    }
                }
            }
        }
}'
```

Update your Amazon Q Business retriever to remove any existing boosts

This example shows how to remove any existing boosts from document attributes in your retriever.

```
aws qbusiness update-retriever \
--application-id APPLICATION-ID --retriever-id RETRIEVER-ID \
--configuration '{
        "nativeIndexConfiguration": {
            "indexId": "INDEX-ID"
        }
}'
```

Get details about your Amazon Q Business retriever boosts

This example shows how to get details for your existing boosting configuration

```
aws qbusiness get-retriever \
--application-id APPLICATION-ID --retriever-id RETRIEVER-ID
```

Enabling document attributes for search in Amazon Q Business

> **Note**
>
> Relevance tuning has replaced metadata boosting. For more information, see Tuning the query results based on document attribute relevancy.

For `STRING` and `STRING_LIST` type attributes to be eligible for boosting, they must first be enabled for search in your Amazon Q index.

The following sections outline how to do so using both the console and the API.

Topics

- Using the console
- Using the API

Using the console

To enable document attributes using the console, use the **Metadata** functionality. The following procedure outlines how.

To create and map document attributes to index fields

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation pane, from **Enhancements**, choose **Metadata controls**.
3. From **Metadata**, choose **Add metadata field**.
4. From the **Add metadata field** dialog box that opens up, do the following:

    a. For **Metadata field name** – Add a name for the metadata field you're adding to the index.

    b. For **Data type** – Select the data type you want to assign to the metadata field.

    c. For **Usage type** – Select **Searchable** to mark your field searchable to end users.

    d. Select **Add** to finish adding the metadata field to your index.

    Repeat the previous step to add create and map more metadata fields. Once you add a metadata field, you can't delete it.

5. To save all the metadata fields you added, select **Save**.

> **Note**
>
> If you leave the page without saving your changes, any metadata fields you added won't be saved.

You can update the searchability of a metadata field at any time.

Using the API

To enable these attributes for search using the API, use the DocumentAttributeConfiguration object of the UpdateIndex API operation.

The following sections provide AWS CLI examples of how to enable document attributes for search.

Topics

- Making reserved document attributes searchable
- Making custom document attributes searchable
- Checking document attribute search activation

Making reserved document attributes searchable

The following is an example of how to use the AWS CLI to enable for search the `STRING` type reserved document attribute `_category` and the `STRING_LIST` type reserved document attribute `_authors` by using the UpdateIndex API operation.

```
aws qbusiness update-index \
--application-id APPLICATION_ID \
--index-id INDEX_ID \
--document-attribute-configurations '
          [
            {
              "name": "_category",
              "type": "STRING",
              "search": "ENABLED"
            },
            {
              "name": "_authors",
```

```
            "type": "STRING_LIST",
            "search": "ENABLED"
          }
        ]'
```

Making custom document attributes searchable

You can also enable custom document attributes for search using the DocumentAttributeConfiguration object of the UpdateIndex API operation.

The following is an example of how to use the AWS CLI to enable for search the custom `STRING` and `STRING_LIST` type document attributes using the UpdateIndex API operation.

```
aws qbusiness update-index \
--application-id APPLICATION_ID \
--index-id INDEX_ID \
--document-attribute-configurations '
         [
           {
             "name": "custom_string",
             "type": "STRING",
             "search": "ENABLED"
           },
           {
             "name": "custom_string_list",
             "type": "STRING_LIST",
             "search": "ENABLED"
           }
           ]'
```

Checking document attribute search activation

To check if a `STRING` or `STRING_LIST` type document attribute has been enabled for search successfully, use the GetIndex API operation.

```
aws qbusiness get-index \
--application-id APPLICATION_ID \
--index-id INDEX_ID
```

The AWS CLI returns the following type of response:

```
{
...
    "documentAttributeConfigurations": [
        {
            "name": "_authors",
            "search": "ENABLED",
            "type": "STRING_LIST"
        },
        {
            "name": "_category",
            "search": "ENABLED",
            "type": "STRING"
        },
        {
            "name": "_created_at",
            "search": "DISABLED",
            "type": "DATE"
        },
        {
            "name": "_data_source_id",
            "search": "ENABLED",
            "type": "STRING"
        },
        {
            "name": "_document_title",
            "search": "ENABLED",
            "type": "STRING"
        },
        {
            "name": "_file_type",
            "search": "ENABLED",
            "type": "STRING"
        },
        {
            "name": "_language_code",
            "search": "ENABLED",
            "type": "STRING"
        },
        {
            "name": "_last_updated_at",
            "search": "DISABLED",
            "type": "DATE"
        },
```

```
        {
            "name": "_source_uri",
            "search": "ENABLED",
            "type": "STRING"
        },
        {
            "name": "_version",
            "search": "ENABLED",
            "type": "STRING"
        },
        {
            "name": "_view_count",
            "search": "DISABLED",
            "type": "NUMBER"
        }
    ],
...
}
```

Configuring metadata controls in Amazon Q Business

Note

Relevance tuning has replaced metadata boosting. For more information, see Tuning the query results based on document attribute relevancy.

Important

This section assumes that you understand document attributes in Amazon Q Business.

Note

Before you configure relevance tuning, you must create a Amazon Q Business retriever and index for your application.

An Amazon Q Business index has fields you can map your document attributes to. Once mapped to document attributes and search enabled, these index fields can be used by admin to boost results from specific sources, or by end users to filter and scope their chat results to specific data.

Mapping document attributes from your documents to index fields is a multi-step process that depends on the document upload method you use.

> **Note**
>
> You can filter using document attributes in chat only through the API. You can boost search results using document attributes on both the console and the API.

Topics

- Mapping document attributes directly to index fields
- Mapping data source document attributes to index fields
- Ingesting attributes using the BatchPutDocument API operation
- Using aggregations and dynamic filtering in chat

Mapping document attributes directly to index fields

When you use the console or the API to directly add documents to your application, you must first create and map your document attributes to index fields before you can use them for filtering in chat or boosting responses. You use the following processes to map document attributes to your index field and mark them searchable.

> **Important**
>
> You can map up to 50 document attributes to index fields. You can mark up to 30 index fields searchable.

Topics

- Using the console
- Using the API

Using the console

To map document attributes to index fields using the Amazon Q Business console, complete the following steps:

To create and map document attributes to index fields

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the left navigation pane, from **Enhancements**, choose **Metadata controls**.
3. From **Metadata**, choose **Add metadata field**.
4. From the **Add metadata field** dialog box that opens up, do the following:

    a. For **Metadata field name** – Add a name for the metadata field you're adding to the index.

    b. For **Data type** – Select the data type you want to assign to the metadata field. Supported data types include **String**, **String list**, **Long (numeric)**, and **Date**.

    c. For **Usage type** – Select **Searchable** to mark your field searchable to end users.

    d. Select **Add** to finish adding the metadata field to your index.

    Repeat the previous step to add create and map more metadata fields. Once you add a metadata field, you can't delete it.
5. To save all the metadata fields you added, select **Save**.

> **Note**
>
> If you leave the page without saving your changes, any metadata fields you added won't be saved.

Any metadata you add and mark searchable can be viewed from the **Metadata** summary. You can update the searchability of a metadata field at any time.

Using the API

To map document attributes to index fields using the Amazon Q Business API, complete the following steps:

1. You create an index by calling the CreateIndex API operation.

2. Then, you create index fields using the UpdateIndex operation. You use this method to map both reserved and custom document attributes to index fields.
3. Optionally, you can test and view the index fields that you've added by using the GetIndex operation.
4. Then, when you use the BatchPutDocument operation to ingest documents into your index, Amazon Q Business extracts your reserved or custom document attributes and maps them to the index fields that you have already created.
5. To mark mapped attributes searchable, follow the steps outlined in enabling attributes for search using APIs.

After you map document attributes directly to index fields using the API, you can select specific attributes for your end user to use for filtering chat responses. With the `UpdateIndex` API operation, you add custom fields or attributes using the `documentAttributeConfigurations` parameter.

The following JSON example uses `documentAttributeConfigurations` to add a field called "Department" to the index.

```
"DocumentmetadataConfigurationUpdates": [
   {
       "Name": "Department",
       "Type": "STRING_VALUE"
   }
]
```

Mapping data source document attributes to index fields

If you use an Amazon Q Business data source connector, you can map default document attributes attached to documents in your data source to fields in your Amazon Q Business index during data source configuration. You can use these document attributes to help your end user filter and scope chat responses.

> **Important**
>
> Filtering using data source document attributes in chat is only supported through the API.

Each data source connector is designed to automatically crawl and map specific document attributes as default from your data source. For example, if you have a field in your data source named `dept` that contains department information for a document, your data source may automatically map it to an index field named `Department`. You can't change or customize default data source attributes that are mapped to an index.

If you use the console, you select and map default field mappings or create and map custom mappings when you configure your connector. On the console, if a default field or a default field property can't be edited, it will appear grayed out. If you use the API, you use the `configuration` parameter of the CreateDataSource API operation to map default document attributes in your data source to index fields.

You can also map any custom document attributes in your data source connector to Amazon Q Business reserved fields. For example, if your data source has a custom attribute named `creation_date`, you can map this field to the equivalent Amazon Q reserved field named `_created_at`. You can also choose to add custom document attributes and map them to custom fields that you create in your index. You do this when you configure and update your data source, using both the console and the API.

If you want to map custom document attributes in your data source to Amazon Q index fields, use the `DocumentAttribute` parameter of the UpdateIndex operation to first create the custom field matching the custom document attribute. By doing so, you can specify and map your reserved or custom data source document attribute to a reserved or custom index field.

Any metadata you add can be viewed and marked searchable using **Metadata controls** or using the API. You can update the searchability of a metadata field at any time.

> **Note**
>
> Document attributes mapped to index fields during the data source configuration process must be enabled for search before they can be used for search accuracy improvements, filtering search results, and metadata boosting.

Most data sources support custom field mappings and follow a specific configuration format, except Amazon S3 and database data sources. The following outlines how Amazon S3 and database data sources configure mappings:

- If you store your documents in an Amazon S3 bucket or Amazon S3 data source, you can either use the console to specify field mappings or specify fields using a JSON metadata file.

  When you use an Amazon S3 bucket as a data source for your index, you use companion metadata files to add metadata to the documents. You place the metadata JSON files in a directory structure that is parallel to your documents. For more information, see S3 document metadata.

  You specify custom fields or attributes in the `Attributes` JSON structure. You can create up to 50 custom fields or attributes. The following example uses `Attributes` to define three custom fields or attributes and one reserved field.

```
"Attributes": {
        "brand": "Amazon Basics",
        "price": 1595,
        "_category": "sports",
        "subcategories": ["outdoors", "electronics"]
    }
```

- For database data sources, if the name of the database column matches the name of a reserved field, the field and column are mapped automatically.

Ingesting attributes using the BatchPutDocument API operation

When you use the BatchPutDocument API operation to add a document to your index, you can specify document attributes—both reserved and custom—as part of `Attributes`. You can add multiple fields or attributes when you call the API operation. You can create up to 50 custom fields or attributes. The following example is a custom field or attribute that adds "Department" to a document.

```
"Attributes":
    {
        "Department": "HR",
        "_category": "Vacation policy"
    }
```

Using aggregations and dynamic filtering in chat

> **Note**
>
> Using aggregations and dynamic filtering in chat is only supported in **Advanced search**.

> **Warning**
>
> To ensure optimal performance and accuracy, perform a `FORCED_FULL_CRAWL` on your data source first before using the features.

Supported aggregations

The Amazon Q API supports the following aggregations:

1. `SUM`: Logic to perform a summation upon any numeric data field. For example, "What is the total sum of tickets in status Open?"
2. `AVERAGE`: Logic to perform an average upon any numeric data field. For example, "What is my average watcher amount for the last week?"
3. `COUNT`: Logic to perform a distinct count of unique values across any type of data field. For example, "Give me the count of unique customer names in the sales database."
4. `LIST_ALL`: Logic to gather a subset of available values for any field. For example, "List all reports on Sunday Sales ticket repository."

Using the mathematical aggregations, users can quickly gather statistical and analytical queries on any data in their data source.

Filtering and Sorting

Amazon Q also offers the ability to intelligently ascertain user intent and apply filtering or sorting across any number of fields. For example, users can query against specific time ranges, values, or string matches by text alone. Sorting can also be inferred through text, for example, "Show me the top 5 accounts sorted by sales data from the last month."

Customizing an Amazon Q Business web experience

Creating an Amazon Q Business application environment automatically creates a web experience with a shareable URL. Amazon Q offers customization options for your web experience, allowing you to align the interface with your organization's branding and user needs. This guide will walk you through the process of customizing text elements, visual themes, and some accessibility features, helping you create a more suited experience for your users.

> **Note**
>
> As of Oct 31, 2024, once you have created a new Amazon Q Business application environment, the default web experience will allow users to interact directly with the LLM to get answers from its general knowledge or uploaded file content, even if the Admin has not yet connected any enterprise data sources.
> For existing application environments, the *Allow direct access to LLM* setting will remain as previously configured. For new application environments, the *Allow direct access to LLM* setting will be enabled by default, though Admins can still disable this if desired.

You can customize a web experience by using either the AWS Management Console or the Amazon Q API. These customizations persist even in *Amazon Q embedded*. You can perform these customizations using either the AWS Management Console or the Amazon Q API (available via the AWS SDK, REST API, and AWS CLI).

If you use the API, customizing your Amazon Q Business can involve a combination of the following API operations.

- CreateApplication – Creates an Amazon Q application environment.
- CreateWebExperience – Creates an Amazon Q web experience.
- GetWebExperience – Gets the properties of the web experience that you set up.
- UpdateWebExperience – Updates the properties of an existing Amazon Q web experience.
- ListWebExperiences – Lists Amazon Q web experiences.

Topics

- Customization overview

- Customizing text elements
- Customizing visual themes
- Reference materials for customizing the visual theme

Customization overview

Creating an Amazon Q Business application environment automatically generates a web experience with a shareable URL. Before sharing this URL, you can customize various elements:

- Title and subtitle
- Welcome message
- Sample prompts
- Logo and favicon
- Colors and fonts

Customizing text elements

This topic shows how to customize text elements using the AWS Management Console and the AWS CLI.

> **Note**
>
> When using the console, you can preview changes in real-time as you customize your web experience.

Topics

- Using the AWS Management Console
- Using the AWS CLI

Using the AWS Management Console

The following procedure shows how to update text elements using the console.

1. Sign in to the AWS Management Console and find the Amazon Q Business console.

2. From the Amazon Q Business **Applications** page, select *your application*, then choose **Customize web experience**.
3. In the **Customize web experience** section, choose **Customize web experience** from the right navigation panel.
4. Choose **Text** and enter the following information:
   - **Title**: A title for your web experience (visible to end users).
   - **Subtitle** (optional): Additional information for end users.
   - **Welcome message**: An optional message for end users (consider mentioning data sources and application capabilities).
   - **Display sample prompts**: Enable or disable the display of sample prompts for the end user's conversation start screen.
5. Choose **Save**.

Using the AWS CLI

The following code snippet shows how to customize text elements using the AWS CLI.

```
aws qbusiness update-web-experience \
--application-id application-id \
--web-experience-id web-experience-id \
--title optional-title \
--subtitle optional-subtitle \
--welcome-message optional-welcome-message \
--sample-prompts-control-mode ENABLED
```

Customizing visual themes

This topic shows how to customize the visual theme using the Amazon Q Business console and the AWS CLI.

Note

- The console only supports accessing customization artifacts stored in Amazon S3 but the Amazon Q Business API supports accessing artifacts in both S3 and other data sources.

- Your web customization artifacts must be of one of the following supported content types.
  - Custom logo and favicons — `image/svg+xml`, `image/x-icon`, and `image/png`. Logo files must be 1 MB or smaller.
  - Custom fonts — `font/ttf`, `font/otf`, `font/woff`, and `font/woff2`.

Topics

- Prerequisites for accessing your customization artifacts stored in Amazon S3
- Using the AWS Management Console
- Using the AWS CLI

Prerequisites for accessing your customization artifacts stored in Amazon S3

1. All S3 URIs for files to read and folders to store must be located in the same AWS Region as the application environment of the web experience.
2. You can use public or private Amazon S3 buckets to save and store your web experience customization.
   - **Prerequisites for public S3 buckets**
     - Ensure all S3 URIs for files to read and folders to store are publicly accessible. For managing access to your S3 files, see Access Control in Amazon S3.
     - Configure CORS to allow console and web app access to resources. For more information, see Configuring cross-origin resource sharing (CORS).
   - **Prerequisites for private S3 buckets**

     To allow Amazon Q Business to access web customization artifacts from your private S3 buckets, you must do the following:
     - Disable access control lists (ACLs). For more information, see Setting Object Ownership on an existing bucket.
     - If your Amazon S3 bucket is encrypted using AWS KMS Key instead of Amazon S3 managed key, a similar resource policy to the sample bucket policy below must be added to AWS KMS key.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "PolicyForAmazonQWebAccessForWebExperienceArtifacts",
        "Effect": "Allow",
        "Principal": {
            "Service": "application.qbusiness.amazonaws.com"
        },
        "Action": ["kms:Decrypt"],
        "Resource": ["arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"]
    }]
}
```

- Create a bucket policy in your private bucket.

> **Note**
>
> The value of "`aws:Referer`" cannot contain "`https://`" or end with "`/`".

Example policy for giving Amazon Q Business access to your web experience artifacts

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "PolicyForAmazonQWebAccessForWebExperienceArtifacts",
            "Effect": "Allow",
            "Principal": {
                "Service": "application.qbusiness.amazonaws.com"
            },
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::amzn-s3-demo-bucket/web-experience-object-
key",
                "arn:aws:s3:::amzn-s3-demo-bucket/web-experience-object-
key-2"
            ],
            "Condition":{
                "StringLike":{
                    "aws:Referer":[
                        "web-experience-domain-without-https"
                    ]
                },
                "Bool": {
                    "aws:SecureTransport": "true"
                }
            }
        }
    ]
}
```

Using the AWS Management Console

The following procedure shows how to customize visual themes using the console.

1. Sign in to the AWS Management Console and find the Amazon Q Business console.
2. From the Amazon Q Business **Applications** page, select *your application*, then choose **Customize web experience**.
3. In the **Customize web experience** section, choose **Customize web experience** from the right navigation panel and choose **Theme**.
4. Choose either **Managed theming** (for direct input of colors and assets) or **Custom theming** (for using your own CSS).
   a. For **Managed theming**:
      - Enter colors for background, and primary title.
      - Provide the S3 URI for the logo file. Logo files must be 1 MB or smaller.
   b. For **Custom theming**:
      - Enter your CSS snippet in the editor.
5. Enter the S3 URI to store your customization.
6. Choose **Save**.

Using the AWS CLI

The following code snippet shows how to customize visual themes using the AWS CLI.

```
aws qbusiness update-web-experience \
--application-id application-id \
--web-experience-id web-experience-id \
--customization-configuration {"customCSSUrl":"custom css url","logoUrl":"logo
 url","fontUrl":"font url","faviconUrl":"favicon url"}
```

Reference materials for customizing the visual theme

Topics

- Color considerations for accessibility
- Choosing Color Values for Your Theme
- Supported Root CSS Variables
- Example

Color considerations for accessibility

When customizing your Amazon Q web experience, it's crucial to prioritize accessibility. Ensure sufficient contrast is there between the text and background colors. Use tools like the WebAIM Contrast Checker to verify your color choices meet Web Content Accessibility Guidelines (WCAG) 2.x standards.

For comprehensive accessibility guidelines, refer to the Web Content Accessibility Guidelines (WCAG).

Choosing Color Values for Your Theme

Amazon Q supports the following color value formats:

- Hexadecimal colors (with and without transparency)
- RGB and RGBA colors

- HSL and HSLA colors
- Predefined/Cross-browser color names

> **Note**
>
> Amazon Q Business doesn't support `currentcolor`. For a comprehensive list of supported CSS color values, see W3Schools CSS Colors

Supported Root CSS Variables

Only the following root CSS variables are supported:

```
--black
--white
--foreground
--primary
--primary-foreground
--secondary
--secondary-foreground
--card
--card-foreground
--popover
--popover-foreground
--tooltip
--tooltip-foreground
--muted
--muted-foreground
--accent
--accent-foreground
--info
--info-foreground
--success
--success-foreground
--warning
--warning-foreground
--error
--error-foreground
--destructive
--destructive-foreground
--border
```

```
--input
--ring
--radius

--background
--qbusiness-webexperience-title-color
--qbusiness-webexperience-font-typeface
--qbusiness-webexperience-chat-user-background-color
--qbusiness-webexperience-chat-user-text-color
--qbusiness-webexperience-chat-agent-background-color
--qbusiness-webexperience-chat-agent-text-color
--qbusiness-webexperience-chat-logo-visibility
--qbusiness-webexperience-logo-url
--qbusiness-webexperience-font-url
--qbusiness-webexperience-favicon-url
```

Example

CSS

The following is an example of a valid CSS file setting the visual theme for Amazon Q Business.

```
:root {
  --background: #FFFFFF;
  --qbusinesness-webexperience-title-color: #9013FE;
  --qbusiness-webexperience-font-typeface: Custom Font;
  --qbusiness-webexperience-chat-user-background-color: #7ED321;
  --qbusiness-webexperience-chat-user-text-color: #344054;
  --qbusiness-webexperience-chat-agent-background-color: #FFFFFF;
  --qbusiness-webexperience-chat-agent-text-color: #344054;
  --qbusiness-webexperience-chat-logo-visibility: hidden;
  --qbusiness-webexperience-logo-url: "https://<bucket_name>.s3.<region>.amazonaws.com/
<logo_name>.png";
  --qbusiness-webexperience-font-url: "https://<bucket_name>.s3.<region>.amazonaws.com/
<font_name>.ttf";
  --qbusiness-webexperience-favicon-url: "https://
<bucket_name>.s3.<region>.amazonaws.com/<favicon_name>.ico";
}
```

Configuring actions in Amazon Q Business

After you configure your application environment, you can optionally choose to add integrations to third-party services using Amazon Q Business plugins. Plugins enable your end users to perform specific tasks in third-party services—such as change status of a ticket, or view open incidents—from within their web experience chat. You can integrate with one of the built-in plugins, or use custom plugins to create your own integrations.

Amazon Q Business offers plugins to enhance your application's functionality. Plugins help streamline tasks and boost productivity by integrating external services into the Amazon Q Business chat interface.

Amazon Q Business supports two types of plugins: built-in plugins and custom plugins.

- **Fully integrated plugins** – The Quick plugin is fully integrated with Amazon Q Business, and won't appear in the list of plugins in the web experience. This plugin gives an Amazon Q Business application access to insights and external databases through Amazon Quick. For more information, see Using the Quick plugin to get insights from structured data.
- **Built-in plugins** – These plugins are pre-made for popular services like Jira, Salesforce, ServiceNow, and Zendesk. They allow users to perform tasks in these services directly from their Amazon Q Business chat. For example, an IT representative can create a ServiceNow incident without leaving the chat.
- **Custom plugins** – These plugins let you connect Amazon Q Business with any third-party application. Users can then use natural language to access real-time data or perform actions in these applications.

> **Note**
>
> You can have up to 25 plugins for each application environment. Each plugin should serve a different purpose. You can activate, deactivate, edit, or delete plugins as needed.

Topics

- Using the Quick plugin to get insights from structured data
- Built-in plugins for Amazon Q Business

- Custom plugins for Amazon Q Business
- Managing Amazon Q Business plugins

Using the Quick plugin to get insights from structured data

> **Note**
>
> The Quick plugin feature is in preview and is subject to change.

The Quick plugin is a fully integrated plugin that gives an Amazon Q Business application access to insights and external databases through Amazon Quick. Quick is a business intelligence service that provides insights from your structured data, such as databases, data lakes, and data warehouses.

With the Quick plugin for Amazon Q Business, end users can get answers from this structured data directly in an Amazon Q Business application. You don't have to index or reformat this structured data, and you don't need to migrate it to Amazon Q Business.

For example, an end user might ask "What was the revenue per month for my business for 2023?" in their Amazon Q Business chat application. They would get answers based on your unstructured data in Amazon Q Business and, below this response, Quick answers based on structured data.

The response from QuickSight can include a multi-visual answer that includes an AI-generated narrative that summarizes key insights, and supporting visuals and interactive graphs to add context. If these visuals don't exist already, Quick can generate them on the fly based on the user's question and the available data in Quick and external databases.

To enable the plugin, you use Amazon Q Business to link your Amazon Quick account with your application and grant it permission to communicate with Quick. If you use the console, you can create the Quick account in Amazon Q Business. If you already have a Quick account, you can enable the plugin with the console or the CreatePlugin API operation.

After you create resources in Quick (including datasets, topics, and, optionally, dashboards), end users automatically start getting insights based on your structured data.

Important

The Quick plugin is fully integrated with Amazon Q Business, and won't appear in the list of plugins in the web experience. For every user prompt, it automatically queries Quick. For information about pausing the plugin, see Pausing integration with Quick.

Note

If your Admin controls and guardrails settings allow Amazon Q to automatically orchestrate end user chat queries across plugins and data sources, an Quick plugin will only activate if:

- No other plugin actions (read or write requests requiring additional end user input through forms) are detected, or, in progress.
- No end user authentication requests are pending.

Topics

- Pricing
- Guidelines and requirements
- Service access role
- Configuring an Amazon Q Business application to use the plugin
- Getting data insights from Amazon Quick answers
- Pausing integration with Quick

Pricing

When you set up the integration with Quick, you assign one or more IAM Identity Center groups the Quick Admin Pro role. This role grants users access to all Generative BI capabilities in Amazon Quick. Your Quick administrator is responsible for adding and managing user permissions and configuring your Quick account.

The Quick Admin Pro role incurs additional costs. For more information about pricing, see Amazon Quick pricing. For more information about Pro roles in Amazon Quick, see Get started with Generative BI.

When you link a Quick account and an Amazon Q Business application, the following groups get Pro subscription benefits at no additional cost:

- Quick Admin Pro groups are added to the Amazon Q Business Pro subscription.
- Existing Amazon Q Business Pro groups are assigned the Quick Reader Pro role.

Guidelines and requirements

- You must use IAM Identity Center for authentication for both Quick and Amazon Q Business. If your Amazon Q Business application doesn't use IAM Identity Center, you must create a new one that does. For information about creating an IAM Identity Center integrated application, see Configuring an Amazon Q Business application using AWS IAM Identity Center.
- Your Amazon Q Business application and Amazon Quick account must be in the same AWS Region.
- To get answers from QuickSight in your web experience, you must add at least one index to your Amazon Q Business application. To learn how to add an index, see creating an index.
- If you don't have a Quick account, you can create the account from the Amazon Q Business console when you configure your application to communicate with Quick.
- You must authorize Amazon Q Business to communicate with Amazon Quick with a service role. For more information, see Service access role.
- The IAM role for your Amazon Q Business web experience must have `quicksight:GenerateEmbedUrlForRegisteredUserWithIdentity` permissions. For a policy example, see IAM role for an Amazon Q Business web experience using IAM Identity Center.

Service access role

When you link your Quick account in the Amazon Q Business console, you specify an AWS Identity and Access Management (IAM) role that authorizes Amazon Q Business to communicate with Amazon Quick. In the console, you can choose to create this role with the correct permissions automatically configured. Or you can manually create it.

- The role's permissions policy must grant `quicksight:PredictQAResults` for Amazon Quick topics and, if you create them, dashboards. For a permissions policy example, see AWS managed policy: QBusinessQuicksightPluginPolicy.

- The role's trust policy must grant Amazon Q Business `AssumeRole` and `SetContext`permissions as follows.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessQuicksightManagedPolicyTrustPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "qbusiness.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
                }
            }
        }
    ]
}
```

Configuring an Amazon Q Business application to use the plugin

You configure an Amazon Q Business application to get insights from Quick answers in different ways depending on whether you have a Quick account.

- If you don't have a Quick account, you can create one in the Amazon Q Business console, and then authorize Amazon Q Business to communicate with Quick.
- If you already have a Quick account, you use the Amazon Q Business console or APIs to authorize Amazon Q Business to communicate with Amazon Quick.

After you configure your application, you create Quick datasets, and create and share Quick topics. Users can also get insights from Quick dashboards.

- You can create datasets from new or existing data sources in Amazon Quick. You can use a variety of database data sources to provide data to Amazon Quick. For more information, see Creating datasets.
- Quick *topics* are collections of one or more datasets that represent a subject area that your business users can ask questions about. For more information, see Working with Amazon Quick Q topics.
- A Quick *dashboard* is a read-only snapshot of an analysis that you can share with other Amazon Quick users for reporting purposes. For more information, see Sharing and subscribing to data in Amazon Quick.

Topics

- Creating a new Amazon Quick account in the Amazon Q Business console
- Linking an existing Quick account

Creating a new Amazon Quick account in the Amazon Q Business console

If you don't have an existing Quick account, you can use the Amazon Q Business console to create one and link the two accounts. Then you configure your Quick resources to start getting insights.

To link a new Quick account

1. Log in to the Amazon Q Business console.
2. In **Applications**, choose the name of your application from the list of applications.
3. In the navigation pane, choose **Amazon Quick**.
4. Choose **Create Quick Account**.
5. Give your new account a name, and specify the email address to use for account notifications.
6. Optionally, specify an email for product updates.
7. In **Assign Quick Admin Pro role**, choose the IAM Identity Center groups to assign the Quick Admin Pro role, and choose **Next**.
8. In **Service access**, create a new service role or use an existing one. This role authorizes Amazon Q Business to communicate with Amazon Quick. For more information, see Service access role.
9. Choose **Authorize**.

10. Choose **Go to Quick** to go to your Quick account. There you create datasets, create and share Quick topics, and optionally create, publish, and share dashboards. After you configure these resources, end users start getting insights with Quick answers.

Linking an existing Quick account

If you have an existing Quick account that uses AWS IAM Identity Center for authentication, you can authorize Amazon Q Business to communicate with Amazon Quick in the console or with the Amazon Q Business API. Then end users can start getting insights from new and existing Quick topics and dashboards.

Using the console

If you have an existing Quick account that uses AWS IAM Identity Center for authentication, you can start getting insights after you authorize Amazon Q Business to communicate with Amazon Quick. To authorize Amazon Q Business, you use the Amazon Q Business console to assign IAM Identity Center groups the Admin Pro role. Then you specify a service role that grants Amazon Q Business access.

To link an existing Quick account

1. Log in to the Amazon Q Business console.
2. Choose your application.
3. In the navigation pane, choose **Amazon Quick**.
4. Choose **Authorize Quick answers**.
5. In **Assign Quick Admin Pro role**, choose the IAM Identity Center groups to assign the Admin Pro role. The Quick Admin Pro role includes additional costs. For more information, see Amazon Quick pricing.
6. In **Service access**, create a new service role or use an existing one. This role authorizes Amazon Q Business to communicate with Amazon Quick. For more information, see Service access role.
7. Choose **Authorize**. After you authorize the connection, end users start getting insights from existing Quick resources.
8. To get insights from additional structured data resources, choose **Go to Quick** to go to your Quick account. There you can create additional datasets, topics, and dashboards.

Using the API

To authorize Amazon Q Business with the API, you first use IAM Identity Center to assign groups the Admin Pro role. Also, if your Quick account was created before November 25, 2024 and uses IdC authentication, use the UpdateApplicationWithTokenExchangeGrant API to update your subscription to allow integration with Amazon Q Business Then you use the CreatePlugin API operation to create a Quick plugin for an Amazon Q Business application.

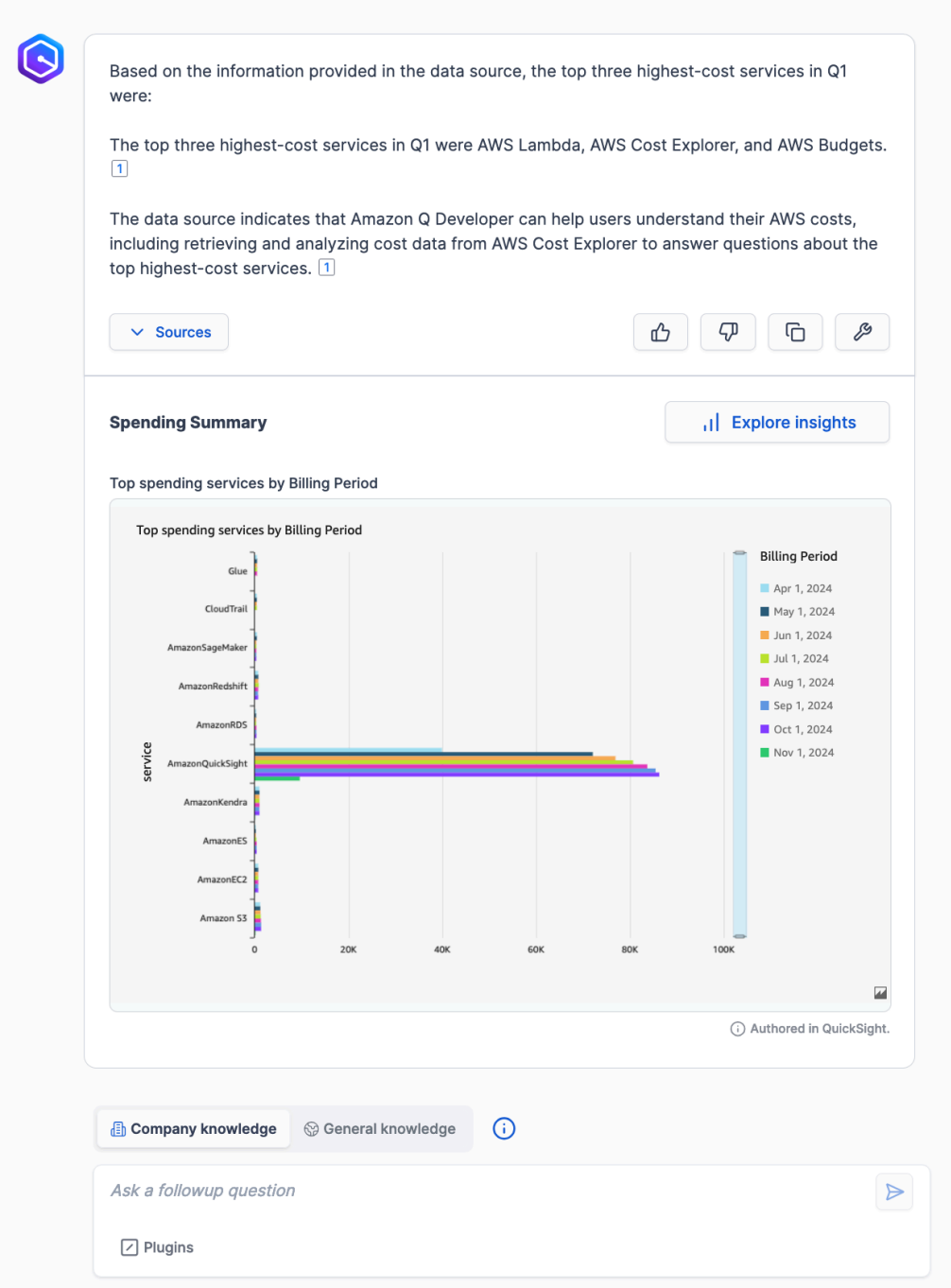
The following code shows how to create a Quick plugin. For `idcApplicationArn`, specify the Amazon Resource Name (ARN) of your application in IAM Identity Center. For `roleArn`, specify an AWS Identity and Access Management (IAM) role that authorizes Amazon Q Business to communicate with Amazon Quick. For more information about this role, see Service access role.

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type QUICKSIGHT \
--auth-configuration idcAuthConfiguration="{idcApplicationArn=arn:aws:sso::<account-
id>:application/<application-id>,roleArn=arn:aws:iam::<account-id>:role/
AmazonQServiceRole}"
```

Getting data insights from Amazon Quick answers

After you complete Configuring the plugin, end users automatically start getting insights from Quick as they submit queries. Unlike other plugins in Amazon Q Business, you don't have to enable Quick insights for end users.

The following example shows the results of a query with Quick answers enabled. It shows a response from Amazon Q Business and a Quick dashboard visual. To navigate to Quick and view details for the insights, choose **Explore insights**.



Pausing integration with Quick

After you enable the plugin, it automatically queries Amazon Quick for every user prompt. To stop automatically querying Quick, you can pause the plugin. When you pause the plugin, end users will no longer see insights from Quick answers. You continue to incur costs for Quick Admin Pro subscription users.

To pause the integration

1. Log in to the Amazon Q Business console.
2. Choose your application.
3. In the navigation pane, choose **Amazon Quick**.
4. In **QuickSight details**, choose **Pause Quick answers**.
5. Confirm your decision to pause the integration. When you're ready to resume, choose **Resume QuickSight Answers** on this page.

Built-in plugins for Amazon Q Business

Built-in plugins have already been built by Amazon Q Business for common use cases across Jira, Salesforce, ServiceNow, and Zendesk. Amazon Q supports the following built-in plugins and actions:

- **Asana** – Create and update tasks.
- **Confluence** – Search pages.
- **Google Calendar** – Find and list events.
- **Jira Cloud** – Read, create, search, and delete issues. Change issue status and move issues to sprint. Create, read, and delete sprints.
- **Microsoft Exchange** – Get events from calendar and get emails.
- **Microsoft Teams** – Send private and public, or channel messages.
- **PagerDuty** – Get incidents, find similar incidents, find root cause incidents, get status updates on incidents, and update incidents, and find out who is on-call for escalation.
- **Salesforce** – Manage cases (create, delete, update, get), Retrieve account lists, handle opportunities (create, update, delete, get, fetch specific), and fetch specific contacts.
- **ServiceNow** – Create, read, delete, and update incidents. Create, update, delete, and read change requests.
- **Smartsheet** – Search and read sheets, and list and get reports.
- **Zendesk Suite** – Create and update tickets, and get ticket details.
- **Jira (Legacy)** – Create an issue.
- **Salesforce (Legacy)** – Create a case.

- **ServiceNow (Legacy)** – Create an incident.
- **Zendesk (Legacy)** – Create a ticket.

This section provides information about how you can use create, configure and use Amazon Q Business built-in plugins.

Topics

- Prerequisites for configuring Amazon Q Business built-in plugins
- Configuring an Asana plugin for Amazon Q Business
- Configuring an Atlassian Confluence plugin for Amazon Q Business
- Configuring a Google Calendar plugin for Amazon Q Business
- Configuring a Jira Cloud plugin for Amazon Q Business
- Configuring a Microsoft Exchange plugin for Amazon Q Business
- Configuring a Microsoft Teams plugin for Amazon Q Business
- Configuring a PagerDuty Advance plugin for Amazon Q Business
- Configuring a Salesforce plugin for Amazon Q Business
- Configuring a ServiceNow plugin for Amazon Q Business
- Configuring a Smartsheet plugin for Amazon Q Business
- Configuring a Zendesk Suite plugin for Amazon Q Business
- Configuring a Jira plugin for Amazon Q Business
- Configuring a Salesforce plugin for Amazon Q Business
- Configuring a ServiceNow plugin for Amazon Q Business
- Configuring a Zendesk plugin for Amazon Q Business
- Using Amazon Q Business built-in plugins

Prerequisites for configuring Amazon Q Business built-in plugins

> **Important**
>
> Built-in plugins require Amazon Q Business Pro subscription. Users with Lite subscriptions cannot access built-in plugin functionality and must upgrade to Pro to use plugins.

Note

If you use the console and are creating a new web experience, Amazon Q Business creates an IAM role with the necessary permissions for you. If you're using the console and choose to use an existing web experience created before December 3, 2024, or you use the API, make sure to add the permissions below.

Before you can configure built-in plugins, make sure you've added the following permissions in you Amazon Q Business web experience's IAM permissions policy:

- In `Action` field for `"Sid": "QBusinessConversationPermissions`, add the following permissions to allow Amazon Q Business to list plugin actions:

```
{
    "Sid": "QBusinessConversationPermissions",
    "Effect": "Allow",
    "Action": [
        "qbusiness:ListPluginActions",
    ],
    "Resource": "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}"
}
```

Add the following permissions to allow Amazon Q Business to allow your end users to discover plugins in their web experience:

```
{
    "Sid": "QBusinessPluginDiscoveryPermissions",
    "Effect": "Allow",
    "Action": [
        "qbusiness:ListPluginTypeMetadata",
        "qbusiness:ListPluginTypeActions"
    ],
    "Resource": "arn:aws:qbusiness:{{region}}:{{account_id}}:application/
{{application_id}}"
}
```

For the complete set of permissions needed for an IAM role, see IAM role for an Amazon Q Business web experience.

- If you use the console or the API to create a plugin, make sure to add the following permissions:

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:111122223333:secret:secret-
id"
            ],
            "Effect": "Allow",
            "Sid": "SecretsManagerPermissions"
        }
    ]
}
```

  To allow Amazon Q to assume a role, use the following trust policy:

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessApplicationTrustPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "qbusiness.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
                }
```

```
            }
        }
    ]
}
```

Configuring an Asana plugin for Amazon Q Business

Asana is a web-based work management platform that helps teams organize, collaborate, and plan tasks. If you're a Asana user, you can create an Amazon Q Business plugin to allow your end users to create and update tasks from within their web experience chat.

To create a Asana plugin, you need configuration information from your Asana instance to set up a connection between Amazon Q and Asana and allow Amazon Q to perform actions in Asana.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites
- Service access roles
- Creating a plugin

Prerequisites

Before you configure your Amazon Q Asana plugin, you must do the following:

- As an admin, create a new OAuth 2.0 Asana app in the Asana developer console with scoped permissions for performing actions in Amazon Q. To learn how to do this, see OAuth in Asana Developer Documentation.
- Make sure you've added following required scopes: `default`, `email`, `openid`, `profile`.
- Select the workspace you want this app to work with under **Choose distribution method**.
- Note the domain URL of your Asana instance. For example: `https://app.asana.com/api/1.0`.
- Note your:
  - **Access token URL** – For Asana OAuth applications, this is `https://app.asana.com/-/oauth_token`.

- **Authorization URL** – For Asana OAuth applications, this is `https://app.asana.com/-/oauth_authorize`.
- **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.
- **Client ID** – The client ID generated when you create your OAuth 2.0 application in Asana.
- **Client secret** – The client secret generated when you create your OAuth 2.0 application in Asana.

You will need this authentication information during the plugin configuration process.

Service access roles

To successfully connect Amazon Q to Asana, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your Asana credentials. Amazon Q assumes this role to access your Asana credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a Asana plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a Asana plugin using the console and code examples for the AWS CLI.

Console

To create a Asana plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **Asana**.

6. For **Asana**, enter the following information:

   a. In **Plugin name**, for **Name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

   b. In **Domain URL**, for **URL** – Enter your Asana domain URL. For example, `https://app.asana.com/api/1.0`.

   c. **OAuth 2.0 authentication** – do the following:

      i. For **AWS Secrets Manager secret** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

      - **Secret name** – A name for your Secrets Manager secret.
      - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Asana.
      - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Asana.
      - For **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.

      ii. For **Access token URL** – For Asana OAuth applications, this is `https://app.asana.com/-/oauth_token`.

      iii. For **Authorization URL** – For Asana OAuth applications, this is `https://app.asana.com/-/oauth_authorize` or the authorization URL provided in the OAuth app.

   d. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure tha your service role has the necessary permissions.

7. **Tags – *optional*** – An optional tag to track your plugin.

8. Choose **Save**.

AWS CLI

To create a Asana plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type ASANA \
--server-url https://app.asana.com/api/1.0 \
--auth-configuration oAuth2ClientCredentialConfiguration="{secretArn=<secret-
arn>,roleArn=<role-arn>,authorizationUrl=<auth-url>,tokenUrl=<token-url>}"
```

Configuring an Atlassian Confluence plugin for Amazon Q Business

Atlassian Confluence is a collaborative work-management tool designed for sharing, storing, and working on project planning, software development, and product management. If you're a Atlassian Confluence user, you can create an Amazon Q Business plugin to allow your end users to search pages from within their web experience chat.

To create a Atlassian Confluence plugin, you need configuration information from your Atlassian Confluence instance to set up a connection between Amazon Q and Atlassian Confluence and allow Amazon Q to perform actions in Atlassian Confluence.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites
- Service access roles
- Creating a plugin

Prerequisites

Before you configure your Amazon Q Atlassian Confluence plugin, you must do the following:

- As an admin, create a new OAuth 2.0 Atlassian Confluence app in the Atlassian Confluence developer console with scoped permissions for performing actions in Amazon Q. To learn how to do this, see OAuth 2.0 (3LO) apps in Atlassian Confluence Developer Documentation. Make sure sharing is enabled. Required scopes: `search:confluence`.

- Note the domain URL of your Atlassian Confluence instance. For example: `https://api.atlassian.com/ex/confluence/`*`yourInstanceId`*. To learn how to retrieve your instance ID (Cloud Site ID), go to How to retrieve Cloud Site Id.
- Note your:
  - **Access token URL** – For Atlassian Confluence OAuth applications, this is `https://auth.atlassian.com/oauth/token`.
  - **Authorization URL** – For Atlassian Confluence OAuth applications, this is `https://auth.atlassian.com/authorize`.
  - **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.
  - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Atlassian Confluence.
  - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Atlassian Confluence.

  You will need this authentication information during the plugin configuration process.

Service access roles

To successfully connect Amazon Q to Atlassian Confluence, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your Atlassian Confluence credentials. Amazon Q assumes this role to access your Atlassian Confluence credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
```

```
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a Atlassian Confluence plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a Atlassian Confluence plugin using the console and code examples for the AWS CLI.

Console

To create a Atlassian Confluence plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **Atlassian Confluence**.
6. For **Atlassian Confluence**, enter the following information:

    a. In **Plugin name**, for **Name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

    b. In **Domain URL**, for **URL** – Enter your Atlassian Confluence domain URL. For example, `https://api.atlassian.com/ex/confluence/`*`yourInstanceId`*.

    c. **OAuth 2.0 authentication** – do the following:

        i. For **AWS Secrets Manager secret** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

        - **Secret name** – A name for your Secrets Manager secret.
        - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Atlassian Confluence.
        - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Atlassian Confluence.
        - For **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.

        ii. For **Access token URL** – For Atlassian Confluence OAuth applications, this is `https://auth.atlassian.com/oauth/token`.

        iii. For **Authorization URL** – For Atlassian Confluence OAuth applications, this is `https://auth.atlassian.com/authorize`.

    d. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure tha your service role has the necessary permissions.

7. **Tags –** ***optional*** – An optional tag to track your plugin.

8. Choose **Save**.

AWS CLI

To create a Atlassian Confluence plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type ATLASSIAN_CONFLUENCE \
--server-url https://api.atlassian.com/ex/confluence/yourInstanceId \
--auth-configuration oAuth2ClientCredentialConfiguration="{secretArn=<secret-
arn>,roleArn=<role-arn>,authorizationUrl=<auth-url>,tokenUrl=<token-url>}"
```

Configuring a Google Calendar plugin for Amazon Q Business

Google Calendar is an online calendar service that helps users schedule meetings, set up events, set reminders, and share their schedules. If you're a Google Calendar user, you can create an Amazon Q Business plugin to allow your end users to find and list events from within their web experience chat.

To create a Google Calendar plugin, you need configuration information from your Google Calendar instance to set up a connection between Amazon Q and Google Calendar and allow Amazon Q to perform actions in Google Calendar.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites
- Service access roles
- Creating a plugin

Prerequisites

Before you configure your Amazon Q Google Calendar plugin, you must do the following:

- As an admin, create a new OAuth 2.0 Google Calendar app in the Google Calendar developer console with scoped permissions for performing actions in Amazon Q. To learn how to do this, see Using OAuth 2.0 to Access Google APIs in Google Calendar Developer Documentation.
- Make sure you've added following required scopes: `calendar.readonly`, `calendar.events`.
- Note the domain URL of your Google Calendar instance. For example: `https://www.googleapis.com/calendar/v3`.
- Note your:
  - **Access token URL** – For Google Calendar OAuth applications, this is `https://oauth2.googleapis.com/token`.
  - **Authorization URL** – For Google Calendar OAuth applications, this is `https://accounts.google.com/o/oauth2/v2/auth`.
  - **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.
  - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Google Calendar.
  - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Google Calendar.

  You will need this authentication information during the plugin configuration process.

Service access roles

To successfully connect Amazon Q to Google Calendar, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your Google Calendar credentials. Amazon Q assumes this role to access your Google Calendar credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
```

```
            "Resource": [
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a Google Calendar plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a Google Calendar plugin using the console and code examples for the AWS CLI.

Console

To create a Google Calendar plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **Google Calendar**.
6. For **Google Calendar**, enter the following information:

    a. In **Plugin name**, for **Name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

    b. In **Domain URL**, for **URL** – Enter your Google Calendar domain URL. For example, `https://www.googleapis.com/calendar/v3`.

    c. **OAuth 2.0 authentication** – do the following:

        i. For **AWS Secrets Manager secret** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

            - **Secret name** – A name for your Secrets Manager secret.
            - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Google Calendar.
            - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Google Calendar.
            - For **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.

        ii. For **Access token URL** – For Google Calendar OAuth applications, this is `https://oauth2.googleapis.com/token`.

        iii. For **Authorization URL** – For Google Calendar OAuth applications, this is `https://accounts.google.com/o/oauth2/v2/auth`.

d. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure tha your service role has the necessary permissions.

7. **Tags – *optional*** – An optional tag to track your plugin.
8. Choose **Save**.

AWS CLI

To create a Google Calendar plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type GOOGLE_CALENDAR \
--server-url https://www.googleapis.com/calendar/v3 \
--auth-configuration oAuth2ClientCredentialConfiguration="{secretArn=<secret-
arn>,roleArn=<role-arn>,authorizationUrl=<auth-url>,tokenUrl=<token-url>}"
```

Configuring a Jira Cloud plugin for Amazon Q Business

Jira Cloud is a project management tool that creates issues (tickets) for software development, product management, and bug tracking. If you're a Jira Cloud user, you can create an Amazon Q Business plugin to allow your end users to perform the following actions from within their web experience chat:

- Read issues
- Create issues
- Search issues
- Change issue status
- Delete issue
- Read sprint
- Move issue to sprint
- Create sprint
- Delete sprint

To create a Jira Cloud plugin, you need configuration information from your Jira Cloud instance to set up a connection between Amazon Q and Jira Cloud and allow Amazon Q to perform actions in Jira Cloud.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites
- Service access roles
- Creating a plugin

Prerequisites

Before you configure your Amazon Q Jira Cloud plugin, you must do the following:

- As an admin, create a new OAuth 2.0 Jira Cloud app in the Jira Cloud developer console with scoped permissions for performing actions in Amazon Q. To learn how to do this, see OAuth 2.0 (3LO) apps in Jira Cloud Developer Documentation.
- Make sure sharing is enabled and the following required scopes are added:
  - `read:jira-work`
  - `write:jira-work`
  - `manage:jira-project`
  - `read:sprint:jira-software`
  - `write:sprint:jira-software`
  - `delete:sprint:jira-software`
  - `read:board-scope:jira-software`
  - `read:project:jira`
- Note the domain URL of your Jira Cloud instance. For example: `https://api.atlassian.com/ex/jira/`*`yourInstanceId`*. To learn how to retrieve your instance ID (Cloud Site ID), go to How to retrieve Cloud Site Id in Jira Software Support.
- Note your:
  - **Access token URL** – For Jira Cloud OAuth applications, this is `https://auth.atlassian.com/oauth/token`.

- **Authorization URL** – For Jira Cloud OAuth applications, this is `https://auth.atlassian.com/authorize`.
- **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.
- **Client ID** – The client ID generated when you create your OAuth 2.0 application in Jira Cloud.
- **Client secret** – The client secret generated when you create your OAuth 2.0 application in Jira Cloud.

You will need this authentication information during the plugin configuration process.

Service access roles

To successfully connect Amazon Q to Jira Cloud, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your Jira Cloud credentials. Amazon Q assumes this role to access your Jira Cloud credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a Jira Cloud plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a Jira Cloud plugin using the console and code examples for the AWS CLI.

Console

To create a Jira Cloud plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **Jira Cloud**.

6. For **Jira Cloud**, enter the following information:

   a. In **Plugin name**, for **Name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

   b. In **Domain URL**, for **URL** – Enter your Jira Cloud domain URL. For example, `https://api.atlassian.com/ex/jira/yourInstanceId`.

   c. **OAuth 2.0 authentication** – do the following:

      i. For **AWS Secrets Manager secret** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

      - **Secret name** – A name for your Secrets Manager secret.
      - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Jira Cloud.
      - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Jira Cloud.
      - For **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.

      ii. For **Access token URL** – For Jira Cloud OAuth applications, this is `https://auth.atlassian.com/oauth/token`.

      iii. For **Authorization URL** – For Jira Cloud OAuth applications, this is `https://auth.atlassian.com/authorize`.

   d. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure tha your service role has the necessary permissions.

7. **Tags – *optional*** – An optional tag to track your plugin.

8. Choose **Save**.

AWS CLI

To create a Jira Cloud plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type JIRA_CLOUD \
--server-url  https://api.atlassian.com/ex/jira/yourInstanceId \
--auth-configuration oAuth2ClientCredentialConfiguration="{secretArn=<secret-
arn>,roleArn=<role-arn>,authorizationUrl=<auth-url>,tokenUrl=<token-url>}"
```

Configuring a Microsoft Exchange plugin for Amazon Q Business

Microsoft Exchange is an enterprise collaboration tool for messaging, meetings, and file sharing. If you're a Microsoft Exchange user, you can create an Amazon Q Business plugin to allow your end users to get events from their calendars and get emails from within their web experience chat.

To create a Microsoft Exchange plugin, you need configuration information from your Microsoft Exchange instance to set up a connection between Amazon Q and Microsoft Exchange and allow Amazon Q to perform actions in Microsoft Exchange.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites
- Service access roles
- Creating a plugin

Prerequisites

Before you configure your Amazon Q Microsoft Exchange plugin, you must do the following:

- As an admin, create a new OAuth 2.0 Microsoft Exchange app in the Microsoft Exchange developer console with scoped permissions for performing actions in Amazon Q. To learn how to do this, see Register an application in Microsoft Exchange Developer Documentation. Select **Accounts** in any organizational directly under **Supported Account Types**.
- Make sure you've added following required scopes: `mail.read`, `mail.send`, `calendars.readwrite`.
- Note the domain URL of your Microsoft Exchange instance. For example: `https://graph.microsoft.com/v1.0`.

- Note your:
  - **Access token URL** – For Microsoft Exchange OAuth applications, this is `https://login.microsoftonline.com/common/oauth2/v2.0/token`.
  - **Authorization URL** – For Microsoft Exchange OAuth applications, this is `https://login.microsoftonline.com/common/oauth2/v2.0/authorize`.
  - **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.
  - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Microsoft Exchange.
  - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Microsoft Exchange.

  You will need this authentication information during the plugin configuration process.

Service access roles

To successfully connect Amazon Q to Microsoft Exchange, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your Microsoft Exchange credentials. Amazon Q assumes this role to access your Microsoft Exchange credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a Microsoft Exchange plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a Microsoft Exchange plugin using the console and code examples for the AWS CLI.

Console

To create a Microsoft Exchange plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.

3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **Microsoft Exchange**.
6. For **Microsoft Exchange**, enter the following information:

    a. In **Plugin name**, for **Name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

    b. In **Domain URL**, for **URL** – Enter your Microsoft Exchange domain URL. For example, `https://graph.microsoft.com/v1.0`.

    c. **OAuth 2.0 authentication** – do the following:

        i. For **AWS Secrets Manager secret** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

            - **Secret name** – A name for your Secrets Manager secret.
            - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Microsoft Exchange.
            - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Microsoft Exchange.
            - For **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.

        ii. For **Access token URL** – For Microsoft Exchange OAuth applications, this is `https://login.microsoftonline.com/common/oauth2/v2.0/token`.

        iii. For **Authorization URL** – For Microsoft Exchange OAuth applications, this is `https://login.microsoftonline.com/common/oauth2/v2.0/authorize`.

    d. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure tha your service role has the necessary permissions.

7. **Tags – *optional*** – An optional tag to track your plugin.
8. Choose **Save**.

AWS CLI

To create a Microsoft Exchange plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type MICROSOFT_EXCHANGE \
--server-url https://graph.microsoft.com/v1.0 \
--auth-configuration oAuth2ClientCredentialConfiguration="{secretArn=<secret-
arn>,roleArn=<role-arn>,authorizationUrl=<auth-url>,tokenUrl=<token-url>}"
```

Configuring a Microsoft Teams plugin for Amazon Q Business

Microsoft Teams is an enterprise collaboration tool for messaging, meetings, and file sharing. If you're a Microsoft Teams user, you can create an Amazon Q Business plugin to allow your end users to send private and public (channel) messages from within their web experience chat.

To create a Microsoft Teams plugin, you need configuration information from your Microsoft Teams instance to set up a connection between Amazon Q and Microsoft Teams and allow Amazon Q to perform actions in Microsoft Teams.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites
- Service access roles
- Creating a plugin

Prerequisites

Before you configure your Amazon Q Microsoft Teams plugin, you must do the following:

- As an admin, create a new OAuth 2.0 Microsoft Teams app in the Microsoft Teams developer console with scoped permissions for performing actions in Amazon Q. To learn how to do this, see Register an application in Microsoft Teams Developer Documentation. Select **Accounts** in any organizational directly under **Supported Account Types**.

- Make sure you've added following required scopes:
  - `channelMessage.send`
  - `chatMessage.send`
  - `Team.ReadBasic.All`
  - `Channel.ReadBasic.All`
  - `Chat.Read`
- Note the domain URL of your Microsoft Teams instance. For example: `https://graph.microsoft.com/v1.0`.
- Note your:
  - **Access token URL** – For Microsoft Teams OAuth applications, this is `https://login.microsoftonline.com/common/oauth2/v2.0/token`.
  - **Authorization URL** – For Microsoft Teams OAuth applications, this is `https://login.microsoftonline.com/common/oauth2/v2.0/authorize`.
  - **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.
  - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Microsoft Teams.
  - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Microsoft Teams.

  You will need this authentication information during the plugin configuration process.

Service access roles

To successfully connect Amazon Q to Microsoft Teams, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your Microsoft Teams credentials. Amazon Q assumes this role to access your Microsoft Teams credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
```

```
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a Microsoft Teams plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a Microsoft Teams plugin using the console and code examples for the AWS CLI.

Console

To create a Microsoft Teams plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **Microsoft Teams**.
6. For **Microsoft Teams**, enter the following information:

    a. In **Plugin name**, for **Name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

    b. In **Domain URL**, for **URL** – Enter your Microsoft Teams domain URL. For example, `https://graph.microsoft.com/v1.0`.

    c. **OAuth 2.0 authentication** – do the following:

        i. For **AWS Secrets Manager secret** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

        - **Secret name** – A name for your Secrets Manager secret.
        - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Microsoft Teams.
        - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Microsoft Teams.
        - For **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens

in this URL. This callback URL needs to be allowlisted in your third-party application.

ii. For **Access token URL** – For Microsoft Teams OAuth applications, this is `https://login.microsoftonline.com/common/oauth2/v2.0/token`.

iii. For **Authorization URL** – For Microsoft Teams OAuth applications, this is `https://login.microsoftonline.com/common/oauth2/v2.0/authorize`.

d. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure tha your service role has the necessary permissions.

7. **Tags – *optional*** – An optional tag to track your plugin.
8. Choose **Save**.

AWS CLI

To create a Microsoft Teams plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type MICROSOFT_TEAMS \
--server-url https://graph.microsoft.com/v1.0 \
--auth-configuration oAuth2ClientCredentialConfiguration="{secretArn=<secret-arn>,roleArn=<role-arn>,authorizationUrl=<auth-url>,tokenUrl=<token-url>}"
```

Configuring a PagerDuty Advance plugin for Amazon Q Business

PagerDuty Operations Cloud is a software-as-a-service (SaaS) incident response management platform that provides IT teams with knowledge about incidents as soon as they occur. If you're a PagerDuty Advance customer who has PagerDuty Advance AI Assistant functionality turned on, you can use the Amazon Q Business PagerDuty Advance plugin to allow your end users to perform the following actions from within their web experience chat:

- Get incidents
- Similar incidents
- Root cause incident
- Find recent changes

- Who is on-call
- Status update on incident
- Customer impact
- Update incident

To create a PagerDuty Advance plugin, you need configuration information from your PagerDuty Advance instance to set up a connection between Amazon Q and PagerDuty Advance and allow Amazon Q to perform actions in PagerDuty Advance.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites
- Service access roles
- Creating a plugin

Prerequisites

Before you configure your Amazon Q PagerDuty Advance plugin, you must do the following:

- As an admin, create a new OAuth 2.0 PagerDuty Advance app in the PagerDuty Advance developer console with scoped permissions for performing actions in Amazon Q. To learn how to do this, see Register an App in PagerDuty Advance Developer Documentation.
- Make sure you've added following required scopes:
  - `openid`
  - `write`

> **Note**
>
> We recommend choosing Classic OAuth Scopes.

- Note the domain URL of your PagerDuty Advance instance. For example: `https://api.pagerduty.com`.
- Note your:

- **Access token URL** – For PagerDuty Advance OAuth applications, this is `https://identity.pagerduty.com/oauth/token`.
- **Authorization URL** – For PagerDuty Advance OAuth applications, this is `https://identity.pagerduty.com/oauth/authorize`.
- **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.
- **Client ID** – The client ID generated when you create your OAuth 2.0 application in PagerDuty Advance.
- **Client secret** – The client secret generated when you create your OAuth 2.0 application in PagerDuty Advance.

You will need this authentication information during the plugin configuration process.

Service access roles

To successfully connect Amazon Q to PagerDuty Advance, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your PagerDuty Advance credentials. Amazon Q assumes this role to access your PagerDuty Advance credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a PagerDuty Advance plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a PagerDuty Advance plugin using the console and code examples for the AWS CLI.

Console

To create a PagerDuty Advance plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.

4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **PagerDuty Advance**.
6. For **PagerDuty Advance**, enter the following information:

    a. In **Plugin name**, for **Name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

    b. In **Domain URL**, for **URL** – Enter your PagerDuty Advance domain URL. For example, `https://api.pagerduty.com`.

    c. **OAuth 2.0 authentication** – do the following:

        i. For **AWS Secrets Manager secret** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

            - **Secret name** – A name for your Secrets Manager secret.
            - **Client ID** – The client ID generated when you create your OAuth 2.0 application in PagerDuty Advance.
            - **Client secret** – The client secret generated when you create your OAuth 2.0 application in PagerDuty Advance.
            - For **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.

        ii. For **Access token URL** – For PagerDuty Advance OAuth applications, this is `https://identity.pagerduty.com/oauth/token`.

        iii. For **Authorization URL** – For PagerDuty Advance OAuth applications, this is `https://identity.pagerduty.com/oauth/authorize`.

    d. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure tha your service role has the necessary permissions.

7. **Tags – *optional*** – An optional tag to track your plugin.
8. Choose **Save**.

AWS CLI

To create a PagerDuty Advance plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type PAGERDUTY_ADVANCE \
--server-url https://api.pagerduty.com \
--auth-configuration oAuth2ClientCredentialConfiguration="{secretArn=<secret-
arn>,roleArn=<role-arn>,authorizationUrl=<auth-url>,tokenUrl=<token-url>}"
```

Configuring a Salesforce plugin for Amazon Q Business

Salesforce is a customer relationship management (CRM) tool for managing customer interactions. If you're a Salesforce user, you can create an Amazon Q Business plugin to allow your end users to perform the following actions from within their web experience chat:

- Managing cases (create, delete, update, get)
- Retrieving account lists
- Handling opportunities (create, update, delete, get, fetch specific)
- Fetching specific contacts

> **Note**
>
> The Salesforce plugin returns a maximum of 5 items per query to manage response size and performance.

To set up this plugin, you'll need configuration details from your Salesforce instance to connect Amazon Q Business with Salesforce.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites
- Service access roles

- Creating a plugin

Prerequisites

Before you configure your Amazon Q Salesforce plugin, you must do the following:

- As an admin, create a new OAuth 2.0 Salesforce app in the Salesforce developer console with scoped permissions for performing actions in Amazon Q. To learn how to do this, see Create a Connected App in Salesforce for OAuth in Salesforce Developer Documentation.
- Make sure to select **Yes** for **Enable Authorization Code and Credential Flow**, **Require Secret for Web Server Flow**, **Require Secret for Refresh Token Flow**, **Enable Token Exchange Flow**, and **Require Secret for Token Exchange Flow**.
- Make sure that the following required scopes are added:
  - `visualforce`
  - `address`
  - `custom_permissions`
  - `open_id`
  - `profile`
  - `refresh_token`
  - `wave_api`
  - `web`
  - `phome`
  - `offline_access`
  - `chatter_api`
  - `id`
  - `api`
  - `eclair_api`
  - `email`
  - `pardot_api`
  - `full`
- Note the domain URL of your Salesforce instance. For example: `https://yourInstance.my.salesforce.com/services/data/v60.0`.

- Note your:
  - **Access token URL** – For Salesforce OAuth applications, this is `https://login.salesforce.com/services/oauth2/token`.
  - **Authorization URL** – For Salesforce OAuth applications, this is `https://login.salesforce.com/services/oauth2/authorize`.
  - **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.
  - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Salesforce.
  - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Salesforce.

You will need this authentication information during the plugin configuration process.

> **Note**
>
> The Require Proof Key for Code Exchange (PKCE) extension option is not supported and it must be disabled in the Salesforce Connector application.

Service access roles

To successfully connect Amazon Q to Salesforce, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your Salesforce credentials. Amazon Q assumes this role to access your Salesforce credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
```

```
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a Salesforce plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a Salesforce plugin using the console and code examples for the AWS CLI.

Console

To create a Salesforce plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **Salesforce**.
6. For **Salesforce**, enter the following information:

    a. In **Plugin name**, for **Name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

    b. In **Domain URL**, for **URL** – Enter your Salesforce domain URL. For example, `https://yourInstance.my.salesforce.com/services/data/v60.0`.

    c. **OAuth 2.0 authentication** – do the following:

        i. For **AWS Secrets Manager secret** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

            - **Secret name** – A name for your Secrets Manager secret.
            - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Salesforce.
            - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Salesforce.
            - For **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.

        ii. For **Access token URL** – For Salesforce OAuth applications, this is `https://login.salesforce.com/services/oauth2/token`.

        iii. For **Authorization URL** – For Salesforce OAuth applications, this is `https://login.salesforce.com/services/oauth2/authorize`.

d. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure tha your service role has the necessary permissions.

7. **Tags – *optional*** – An optional tag to track your plugin.
8. Choose **Save**.

AWS CLI

To create a Salesforce plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type SALESFORCE_CRM \
--server-url https://yourInstance.my.salesforce.com/services/data/v60.0 \
--auth-configuration oAuth2ClientCredentialConfiguration="{secretArn=<secret-
arn>,roleArn=<role-arn>,authorizationUrl=<auth-url>,tokenUrl=<token-url>}"
```

Configuring a ServiceNow plugin for Amazon Q Business

ServiceNow provides a cloud-based service management system to create and manage organization-level workflows, such as IT services, ticketing systems, and support. ServiceNow uses incidents (tickets) to track issues. If you're a ServiceNow user, you can create an Amazon Q Business plugin to allow your end users to perform the following actions from within their web experience chat:

- Create incident
- Read incident
- Update incident
- Delete incident
- Read change request
- Create change request
- Update change request
- Delete change request

To create a ServiceNow plugin, you need configuration information from your ServiceNow instance to set up a connection between Amazon Q and ServiceNow and allow Amazon Q to perform actions in ServiceNow.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites
- Service access roles
- Creating a plugin

Prerequisites

Before you configure your Amazon Q ServiceNow plugin, you must do the following:

- As an admin, create a new OAuth 2.0 ServiceNow app in the ServiceNow developer console with scoped permissions for performing actions in Amazon Q. To learn how to do this, see Create an endpoint for clients to access the instance in ServiceNow Developer Documentation.
- Make sure the OAuth plugin is active and the OAuth activation property is set to true. Required scopes:
  - `read`
  - `write`
  - `useraccount`

  > **Note**
  >
  > We recommend choosing Classic OAuth Scopes.

- Make sure to create an authentication profile by following the steps outlined in ServiceNow Documentation. For **Type**, select **OAuth**. For authentication policy, select **Allow Access Policy**.

  Then, add the authentication profile you created to the REST API access policies for **Table API** and **Change Management** by following steps outlined in Create REST API access policy in ServiceNow Documentation.
- Note the domain URL of your ServiceNow instance. For example: `https://yourInstanceId.service-now.com`.

- Note your:
  - **Access token URL** – For ServiceNow OAuth applications, this is `https://yourInstanceId.service-now.com/oauth_token.do`.
  - **Authorization URL** – For ServiceNow OAuth applications, this is `https://yourInstanceId.service-now.com/oauth_auth.do`.
  - **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.
  - **Client ID** – The client ID generated when you create your OAuth 2.0 application in ServiceNow.
  - **Client secret** – The client secret generated when you create your OAuth 2.0 application in ServiceNow.

  You will need this authentication information during the plugin configuration process.

Service access roles

To successfully connect Amazon Q to ServiceNow, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your ServiceNow credentials. Amazon Q assumes this role to access your ServiceNow credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a ServiceNow plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a ServiceNow plugin using the console and code examples for the AWS CLI.

Console

To create a ServiceNow plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.

4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **ServiceNow**.
6. For **ServiceNow**, enter the following information:

    a. In **Plugin name**, for **Name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

    b. In **Domain URL**, for **URL** – Enter your ServiceNow domain URL. For example, `https://yourInstanceId.service-now.com`.

    c. **OAuth 2.0 authentication** – do the following:

        i. For **AWS Secrets Manager secret** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

        - **Secret name** – A name for your Secrets Manager secret.
        - **Client ID** – The client ID generated when you create your OAuth 2.0 application in ServiceNow.
        - **Client secret** – The client secret generated when you create your OAuth 2.0 application in ServiceNow.
        - For **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.

        ii. For **Access token URL** – For ServiceNow OAuth applications, this is `https://yourInstanceId.service-now.com/oauth_token.do`.

        iii. For **Authorization URL** – For ServiceNow OAuth applications, this is `https://yourInstanceId.service-now.com/oauth_auth.do`.

    d. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure tha your service role has the necessary permissions.

7. **Tags – *optional*** – An optional tag to track your plugin.
8. Choose **Save**.

AWS CLI

To create a ServiceNow plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type SERVICENOW_NOW_PLATFORM \
--server-url https://yourInstanceId.service-now.com \
--auth-configuration oAuth2ClientCredentialConfiguration="{secretArn=<secret-
arn>,roleArn=<role-arn>,authorizationUrl=<auth-url>,tokenUrl=<token-url>}"
```

Configuring a Smartsheet plugin for Amazon Q Business

Smartsheet is an enterprise work management platform that lets users manage projects, programs and processes at scale using sheets, channels, and workspaces. If you're a Smartsheet user, you can create an Amazon Q Business plugin to allow your end users to search and read sheets, and list and get reports from within their web experience chat.

To create a Smartsheet plugin, you need configuration information from your Smartsheet instance to set up a connection between Amazon Q and Smartsheet and allow Amazon Q to perform actions in Smartsheet.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites
- Service access roles
- Creating a plugin

Prerequisites

Before you configure your Amazon Q Smartsheet plugin, you must do the following:

- As an admin, create a new OAuth 2.0 Smartsheet app in the Smartsheet developer console with scoped permissions for performing actions in Amazon Q. To learn how to do this, see the "Register Your App Using Developer Tools" section in OAuth Walkthrough in the Smartsheet Developer Documentation.

- Make sure you've added following required scopes:
  - `readsheet`
  - `writesheet`
- Note the domain URL of your Smartsheet instance. For example: `https://api.smartsheet.com/2.0`.
- Note your:
  - **Access token URL** – For Smartsheet OAuth applications, this is `https://api.smartsheet.com/2.0/token`.
  - **Authorization URL** – For Smartsheet OAuth applications, this is `https://app.smartsheet.com/b/authorize`.
  - **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.
  - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Smartsheet.
  - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Smartsheet.

  You will need this authentication information during the plugin configuration process.

Service access roles

To successfully connect Amazon Q to Smartsheet, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your Smartsheet credentials. Amazon Q assumes this role to access your Smartsheet credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
```

```
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a Smartsheet plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a Smartsheet plugin using the console and code examples for the AWS CLI.

Console

To create a Smartsheet plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **Smartsheet**.
6. For **Smartsheet**, enter the following information:

    a. In **Plugin name**, for **Name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

    b. In **Domain URL**, for **URL** – Enter your Smartsheet domain URL. For example, `https://api.smartsheet.com/2.0`.

    c. **OAuth 2.0 authentication** – do the following:

        i. For **AWS Secrets Manager secret** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

            - **Secret name** – A name for your Secrets Manager secret.
            - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Smartsheet.
            - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Smartsheet.
            - For **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.

        ii. For **Access token URL** – For Smartsheet OAuth applications, this is `https://api.smartsheet.com/2.0/token`.

        iii. For **Authorization URL** – For Smartsheet OAuth applications, this is `https://app.smartsheet.com/b/authorize`.

d. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure tha your service role has the necessary permissions.

7. **Tags – *optional*** – An optional tag to track your plugin.
8. Choose **Save**.

AWS CLI

To create a Smartsheet plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type SMARTSHEET \
--server-url https://api.smartsheet.com/2.0 \
--auth-configuration oAuth2ClientCredentialConfiguration="{secretArn=<secret-
arn>,roleArn=<role-arn>,authorizationUrl=<auth-url>,tokenUrl=<token-url>}"
```

Configuring a Zendesk Suite plugin for Amazon Q Business

Zendesk Suite is a customer relationship management system that helps businesses automate and enhance customer support interactions by creating tickets to track work. If you're a Zendesk Suite user, you can create an Amazon Q Business plugin to allow your end users to create, update, search for, and get ticket details from within their web experience chat.

To create a Zendesk Suite plugin, you need configuration information from your Zendesk Suite instance to set up a connection between Amazon Q and Zendesk Suite and allow Amazon Q to perform actions in Zendesk Suite.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites
- Service access roles
- Creating a plugin

Prerequisites

Before you configure your Amazon Q Zendesk Suite plugin, you must do the following:

- As an admin, create a new OAuth 2.0 Zendesk Suite app in the Zendesk Suite developer console with scoped permissions for performing actions in Amazon Q. To learn how to do this, see Using OAuth authentication with your application in Zendesk Suite Developer Documentation.
- Make sure the following required scopes are added:
  - `tickets:read`
  - `tickets:write, read`
- Note the domain URL of your Zendesk Suite instance. For example: `https://yourInstanceId.zendesk.com`.
- Note your:
  - **Access token URL** – For Zendesk Suite OAuth applications, this is `https://yourInstanceId.zendesk.com/oauth/tokens`.
  - **Authorization URL** – For Zendesk Suite OAuth applications, this is `https://yourInstanceId.zendesk.com/oauth/authorizations/new`.
  - **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.
  - **Client ID** – The unique identifier generated when you create your OAuth 2.0 application in Zendesk Suite.
  - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Zendesk Suite.

  You will need this authentication information during the plugin configuration process.

Service access roles

To successfully connect Amazon Q to Zendesk Suite, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your Zendesk Suite credentials. Amazon Q assumes this role to access your Zendesk Suite credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a Zendesk Suite plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a Zendesk Suite plugin using the console and code examples for the AWS CLI.

Console

To create a Zendesk Suite plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **Zendesk Suite**.
6. For **Zendesk Suite**, enter the following information:

    a. In **Plugin name**, for **Name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

    b. In **Domain URL**, for **URL** – Enter your Zendesk Suite domain URL. For example, `https://yourInstanceId.zendesk.com`.

    c. **OAuth 2.0 authentication** – do the following:

        i. For **AWS Secrets Manager secret** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

        - **Secret name** – A name for your Secrets Manager secret.
        - **Client ID** – The client ID generated when you create your OAuth 2.0 application in Zendesk Suite.
        - **Client secret** – The client secret generated when you create your OAuth 2.0 application in Zendesk Suite.

- For **Redirect URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is <q-endpoint>, use <q-endpoint>/oauth/callback . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.

ii. For **Access token URL** – For Zendesk Suite OAuth applications, this is `https://yourInstanceId.zendesk.com/oauth/tokens`.

iii. For **Authorization URL** – For Zendesk Suite OAuth applications, this is `https://yourInstanceId.zendesk.com/oauth/authorizations/new`.

d. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure tha your service role has the necessary permissions.

7. **Tags – *optional*** – An optional tag to track your plugin.
8. Choose **Save**.

AWS CLI

To create a Zendesk Suite plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type ZENDESK_SUITE \
--server-url https://yourInstanceId.zendesk.com \
--auth-configuration oAuth2ClientCredentialConfiguration="{secretArn=<secret-arn>,roleArn=<role-arn>,authorizationUrl=<auth-url>,tokenUrl=<token-url>}"
```

Configuring a Jira plugin for Amazon Q Business

Jira is a project management tool that creates issues (tickets) for software development, product management, and bug tracking. If you're a Jira user, you can create an Amazon Q Business plugin to allow your end users to create Jira issues from within their web experience chat.

To create a Jira plugin, you need configuration information from your Jira instance to set up a connection between Amazon Q and Jira and allow Amazon Q to perform actions in Jira.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites for creating an Amazon Q Business Jira plugin
- Service access roles
- Creating a plugin

Prerequisites for creating an Amazon Q Business Jira plugin

Before you configure your Amazon Q Jira plugin, you must do the following:

- Set up a new user in your Jira instance with scoped permissions for performing actions in Amazon Q.
- (Optional) Create an API token for the new user that you created.
- Note this user's Jira username and Jira account password (and optionally, their API token). You will need this basic authentication information for creating an AWS Secrets Manager secret during the plugin configuration process.
- Note the base URL of your Jira Cloud instance hosted by Atlassian. For example: `https://yourcompany.atlassian.net`.

Service access roles

To successfully connect Amazon Q to Jira, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your Jira credentials. Amazon Q assumes this role to access your Jira credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
```

```
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a Jira plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure to create a Jira plugin using the console and code examples for the AWS CLI.

Console

To create a Jira plugin

1. Sign in to the AWS Management Console and open the Amazon Q console at https://console.aws.amazon.com/amazonq/business/.
2. In **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **Jira**.
6. For **Jira**, enter the following information:

    a. **Name**, **Plugin name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

    b. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure that your service role has the necessary permissions.

    c. **URL** – The base URL of your Jira Cloud instance hosted by Atlassian. For example: `https://yourcompany.atlassian.net`.

    d. **Authentication** – Choose to **Create and add a new secret** or **Use an existing one**.

    If you choose to create a new secret, a Secrets Manager secret window opens requesting the following information:

    i. **Secret name** – A name for your Secrets Manager secret.

    ii. **Jira username** – The username for your Jira user.

    iii. **Jira password/API token** – The password/API token for your Jira user.
7. **Tags – *optional*** – Add an optional tag to track your plugin.
8. Choose **Save**.

AWS CLI

To create a Jira plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type JIRA \
--server-url https://example.atlassian.net \
```

```
--auth-configuration basicAuthConfiguration="{secretArn=<secret-arn>,roleArn=<role-arn>}"
```

Configuring a Salesforce plugin for Amazon Q Business

Salesforce is a customer relationship management (CRM) tool for managing support, sales, and marketing teams that you can use to create cases (tickets) to track issues. If you're a Salesforce user, you can create an Amazon Q Business plugin to allow your end users to create Salesforce cases from within their web experience chat.

To create a Salesforce plugin, you need configuration information from your Salesforce instance to set up a connection between Amazon Q and Salesforce and allow Amazon Q to perform actions in Salesforce.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites
- Service access roles
- Creating a plugin

Prerequisites

Before you configure your Amazon Q Salesforce plugin, you must do the following:

- Set up a Connected App using the admin role in your Salesforce instance with Client Credentials Flow enabled.
- As an admin, configure an execution user with scoped permissions for performing actions in Amazon Q. For instructions, see Configure a Connected App for the OAuth 2.0 Client Credentials Flow in the Salesforce documentation.
- Note your Salesforce Connected App's consumer key (`client_id`) and your Salesforce Connected App Consumer secret (`client_secret`). You will need this Oauth 2.0 authentication information for creating an AWS Secrets Manager secret during the plugin configuration process.
- Note the Salesforce My Domain URL of your Salesforce organization. For example: `https://yourdomain.my.salesforce.com`.

Service access roles

To successfully connect Amazon Q to Salesforce, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your Salesforce credentials. Amazon Q assumes this role to access your Salesforce credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
```

```
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a Salesforce plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a Salesforce plugin using the console and code examples for the AWS CLI.

Console

To create a Salesforce plugin

1. Sign in to the AWS Management Console and open the Amazon Q console at https://console.aws.amazon.com/amazonq/business/.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **Salesforce**.
6. For **Salesforce**, enter the following information:

    a. **Name**, for **Plugin name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

    b. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure that your service role has the necessary permissions.

    c. **URL** – My Domain URL of your Salesforce organization. For example: `https://yourdomain.my.salesforce.com`

    d. **Authentication** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

i. **Secret name** – A name for your Secrets Manager secret.

ii. **Connected app consumer key** – The consumer key for your Salesforce connected app.

iii. **Connected app consumer secret** – The consumer secret for your Salesforce connected app.

7. **Tags – *optional*** – An optional tag to track your plugin.
8. Choose **Save**.

AWS CLI

To create a Salesforce plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type SALESFORCE \
--server-url //example.my.salesforce.com \
--auth-configuration oAuth2ClientCredentialConfiguration="{secretArn=<secret-
arn>,roleArn=<role-arn>}"
```

Configuring a ServiceNow plugin for Amazon Q Business

ServiceNow provides a cloud-based service management system to create and manage organization-level workflows, such as IT services, ticketing systems, and support. ServiceNow uses incidents (tickets) to track issues. If you're a ServiceNow user, you can create an Amazon Q Business plugin to allow your end users to create ServiceNow cases from within their web experience chat.

To create a ServiceNow plugin, you need configuration information from your ServiceNow instance to set up a connection between Amazon Q and ServiceNow and allow Amazon Q to perform actions in ServiceNow.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites

- Service access roles
- Creating a plugin

Prerequisites

Before you configure your Amazon Q ServiceNow plugin, you must do the following:

- As an admin, set up a new user in your ServiceNow instance with scoped permissions for performing actions in Amazon Q.
- Note your ServiceNow username and ServiceNow password. You will need this basic authentication information for creating an AWS Secrets Manager secret during the plugin configuration process.
- Note the base URL of your ServiceNow instance. For example: `https://yourinstance.service-now.com`.

Service access roles

To successfully connect Amazon Q to ServiceNow, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your ServiceNow credentials. Amazon Q assumes this role to access your ServiceNow credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a ServiceNow plugin for your web experience chat, you can use the AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a ServiceNow plugin using the console and code examples for the AWS CLI.

Console

To create a ServiceNow plugin

1. Sign in to the AWS Management Console and open the Amazon Q console at https://console.aws.amazon.com/amazonq/business/.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.

3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **ServiceNow**.
6. For **ServiceNow**, enter the following information:

    a. **Name**, for **Plugin name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

    b. **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure tha your service role has the necessary permissions.

    c. **URL** – The base URL of your ServiceNow instance. For example: `https://yourinstance.service-now.com`

    d. **Authentication** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

        i. **Secret name** – A name for your Secrets Manager secret.

        ii. **ServiceNow username** – The username for your ServiceNow user.

        iii. **ServiceNow password** – The password for your ServiceNow user.

7. **Tags – *optional*** – An optional tag to track your plugin.
8. Choose **Save**.

AWS CLI

To create a ServiceNow plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type SERVICE-NOW \
--server-url //example.service-now.com \
--auth-configuration basicAuthConfiguration="{secretArn=<secret-arn>,roleArn=<role-arn>}"
```

Configuring a Zendesk plugin for Amazon Q Business

Zendesk is a customer relationship management system that helps businesses automate and enhance customer support interactions by creating tickets to track work. If you're a Zendesk user, you can create an Amazon Q Business plugin to allow your end users to create Zendesk cases from within their web experience chat.

To create a Zendesk plugin, you need configuration information from your Zendesk instance to set up a connection between Amazon Q and Zendesk and allow Amazon Q to perform actions in Zendesk.

For more information on how to use plugins during your web experience chat, see Using plugins.

Topics

- Prerequisites
- Service access roles
- Creating a plugin

Prerequisites

Before you configure your Amazon Q Zendesk plugin, you must do the following:

- As an admin, set up a new user in your Zendesk instance with scoped permissions for performing actions in Amazon Q.
- (Optional) Create an API token for that new user.
- Note your Zendesk username and Zendesk password/API token. You will need this basic authentication information for creating an AWS Secrets Manager secret during the plugin configuration process.
- Note the base URL of your Zendesk instance. For example: `https://yoursubdomain.zendesk.com`.

Service access roles

To successfully connect Amazon Q to Zendesk, you need to give Amazon Q the following permission to access your Secrets Manager secret to get your Zendesk credentials. Amazon Q assumes this role to access your Zendesk credentials.

The following is the service access IAM role required:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
[[secret-id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessApplicationTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "qbusiness.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        },
        "ArnLike": {
          "aws:SourceArn":"arn:aws:qbusiness:{{your-region}}:
{{source_account}}:application/{{application_id}}"
        }
      }
    }
  ]
}
```

If you use the console and choose to create a new IAM role, Amazon Q creates the role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your IAM role contains these permissions.

Creating a plugin

To create a Zendesk plugin for your web experience chat, you can use AWS Management Console or the CreatePlugin API operation. The following tabs provide a procedure for creating a Zendesk plugin using the console and code examples for the AWS CLI.

Console

To create a Zendesk plugin

1. Sign in to the AWS Management Console and open the Amazon Q console at https://console.aws.amazon.com/amazonq/business/.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, choose **Add plugin**.
5. For **Add plugins**, choose **Zendesk**.
6. For **Zendesk**, enter the following information:

    a. **Name**, **Plugin name** – A name for your Amazon Q plugin. The name can include hyphens (-), but not spaces, and can have a maximum of 1,000 alphanumeric characters.

    b. For **Service access** – Choose **Create and add a new service role** or **Use an existing service role**. Make sure that your service role has the necessary permissions.

    c. **URL** – The base URL of your Zendesk instance. For example: `https://yoursubdomain.zendesk.com`

    d. **Authentication** – Choose **Create and add a new secret** or **Use an existing one**. Your secret must contain the following information:

        i. **Secret name** – A name for your Secrets Manager secret.

        ii. **Zendesk username** – The username for your Zendesk user.

        iii. **Zendesk password/API token** – The password/API token for your Zendesk user.

7. **Tags – *optional*** – An optional tag to track your plugin.

8. Choose **Save**.

AWS CLI

To create a Zendesk plugin

```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
--type ZENDESK \
--server-url //example.zendesk.com \
--auth-configuration basicAuthConfiguration="{secretArn=<secret-arn>,roleArn=<role-arn>}"
```

Using Amazon Q Business built-in plugins

After plugins have been configured, you can use them to perform supported actions in your Amazon Q Business web experience chat. This topic provides an overview of how to use plugins.

> **Important**
>
> Once configured, all authorized Amazon Q web experience end users can use plugins to perform supported actions. If a plugin is activated for an application, end users will see an option to **Use a plugin**. If a plugin is deactivated, users won't see an option to use a plugin. If your Admin controls and guardrails settings allow Amazon Q to automatically orchestrate chat queries across plugins and data sources, your plugin actions can be automatically selected by Amazon Q during chat. End user access to plugins can't be customized.

Topics

- Performing a plugin action
- Example plugin action prompts

Performing a plugin action

> **Note**
>
> If your Admin controls and guardrails settings allow Amazon Q to automatically orchestrate end user chat queries across plugins and data sources, plugin actions will be automatically activated by Amazon Q for your end user during chat. In that case, your end user won't have to follow the steps below.

The following describes how to perform a plugin action from within a web experience chat using both the console and the API.

Console

Performing a plugin action

1. Navigate to the deployed web experience URL and sign with your credentials on the login screen.
2. From conversation settings, choose **Use a plugin**.
3. You can choose to enact plugin actions in two ways:
   a. Ask to perform an action directly. For example: Create a Jira ticket for a broken mouse. See Quick create for more details.
   b. Start chatting in your web experience to find answers to your questions. Then choose to include the conversation context in any plugin action that you take. For example: Summarize this conversation and create a Jira ticket. For more information, see Contextual create.
4. In response to your prompt for an action, Amazon Q displays a review form where you fill in the necessary information required to successfully complete an action.
5. To successfully complete the action, you need to submit it. Your web experience will display a success message if the action succeeds, or an error message if the action fails.

API

Performing a plugin action

```
aws qbusiness chat-sync --application-id '${application-id}' \
```

```
--user-message "Create an issue in Jira for broken button in web application" \
--clientToken '${user-oauth-token} ' \
--chat-mode PLUGIN_MODE \
--chat-mode-configuration '{
    "pluginConfiguration": {
        "pluginId":"${plugin-id}"
        }
    }'
```

Example plugin action prompts

There are two ways you can choose to use plugins in your web experience chat, *quick creation* and *contextual creation*.

Topics

- Quick create
- Contextual create

Quick create

Using quick creation you can directly instruct your web experience to perform a plugin action. For example:

- `Create a Zendesk ticket for a broken mouse`
- `Log an incident in ServiceNow for network outage`
- `Cut an issue in Jira for a broken link on a web page`
- `Create a Salesforce case for a missing invoice`

Contextual create

Using contextual creation you can include conversation contexts to create tickets. For example, consider the following example conversation flows:

Example contextual create actions

- Example 1: Create a ServiceNow incident
- Example 2: Create a ZenDesk ticket
- Example 3: Create a Salesforce case

- Example 4: Create a Jira issue

Example 1: Create a ServiceNow incident

- **User prompt 1** – `How to resolve network issues`
- **Amazon Q response** – *Sample response*
- **User prompt 2** – `How to reset my router`
- **Amazon Q response** – *Sample response*
- **User action request** – `Summarize this conversation and create a ServiceNow incident`

Example 2: Create a ZenDesk ticket

- **User prompt 1** – `Compare Amazon Kendra with OpenSearch`
- **Amazon Q response** – *Sample response*
- **User action request** – `Create a Zendesk ticket to migrate to Amazon Kendra`

Example 3: Create a Salesforce case

- **User prompt 1** – `Where is the IT office located`
- **Amazon Q response** – *Sample response*
- **User prompt 2** – `What floor is the office located in`
- **Amazon Q response** – *Sample response*
- **User action request** – `Create a case in Salesforce summarizing this conversation`

Example 4: Create a Jira issue

- **User prompt 1** – `How do I enable auto-scaling in EC2`
- **Amazon Q response** – *Sample response*
- **User prompt 2** – `How do I create an auto-scaling group`
- **Amazon Q response** – *Sample response*
- **User action request** – `Summarize this conversation and create an issue in Jira`

Custom plugins for Amazon Q Business

You can use the Amazon Q Business console or APIs to create custom plugins for your Amazon Q application.

With custom plugins, you can choose to integrate Amazon Q with any third-party application for a variety of different use cases. Once enabled, end users can use natural language to query data (like available calendar slots, stock prices, vacation balance), and take actions (like booking a meeting, submitting vacation time, updating a record).

To create a custom plugin, you need to perform the following steps:

- Configure authentication and network information to connect Amazon Q Business to your third-party application.
- Create or edit an OpenAPI schema outlining the different API operations you want to enable for your custom plugin in JSON or YAML format.

  You can upload the OpenAPI schema file to Amazon S3 or you can paste it in the OpenAPI text editor in the Amazon Q Business console, which will validate your schema. You can configure up to 20 API operations per custom plugin.

Once your custom plugin is deployed, Amazon Q Business will dynamically determine the appropriate APIs to call to accomplish an end user requested task. In order to maximize plugin accuracy, review the best practices for configuring OpenAPI schema definitions for custom plugins.

> **Note**
>
> Creating custom forms with array fields (fields with nested objects inside an array) for custom plugins isn't supported on the console.

Topics

- Prerequisites for Amazon Q Business custom plugins
- Service access roles for Amazon Q Business custom plugins
- Defining OpenAPI schemas for custom plugins
- Best practices for OpenAPI schema definition for custom plugins

- Creating an Amazon Q Business custom plugin
- Using an Amazon Q Business custom plugin

Prerequisites for Amazon Q Business custom plugins

Before you configure your Amazon Q custom plugin, you must ensure you have the following:

- A defined OpenAPI schema in JSON or YAML (maximum size is 1 MB). In order to maximize accuracy with Amazon Q Business custom plugin, follow the best practices for configuring OpenAPI schema definitions for custom plugins.
- If authentication is required to connect Amazon Q to your third-party application, create OAuth authentication credentials. You need to store these authentication credentials in a Secrets Manager secret to connect your third-party application to Amazon Q.

Service access roles for Amazon Q Business custom plugins

To connect Amazon Q Business to third party applications that require authentication, you need to give the Amazon Q role permissions to access your Secrets Manager secret. This will enable an Amazon Q Business custom plugin to access the credentials needed to log in to the third party service.

- Permission to access your Secrets Manager secret to get the credentials you use to log in to the third party service instance you are creating a plugin for.

You don't have to provide this role for custom plugins that don't require authentication.

> **Important**
>
> If you're changing response settings for an Amazon Q application created and deployed before 16 April, 2024, you need to update your web experience service role. For information on service role permissions needed, see IAM role for an Amazon Q web experience. For information on how to update your web experience service role, see Updating a web experience.

The following is the service access IAM role required:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowQBusinessToGetSecretValue",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:111122223333:secret:
[[secret_id]]"
            ]
        }
    ]
}
```

To allow Amazon Q to assume a role, use the following trust policy:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessApplicationTrustPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "qbusiness.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
                }
```

```
            }
        }
    ]
}
```

Amazon Q assumes this role to access your third party service instance credentials.

If you use the console and choose to create a new IAM role, Amazon Q creates the IAM role for you. If you use the console and choose to use an existing secret, or you use the API, make sure your secret contains the permissions above. For more information on creating IAM roles, see Creating IAM roles.

Defining OpenAPI schemas for custom plugins

Amazon Q Business uses the configured third-party OpenAPI specifications to dynamically determine which API operations to perform in order to fulfill an end user requests. To configure a custom plugin you must define at least 1 API operation and a maximum of 20 API operations that can be invoked. To define the API operations, create an OpenAPI schema in JSON or YAML format. You can create OpenAPI schema files and upload them to Amazon Simple Storage Service (Amazon S3). Alternatively, you can use the OpenAPI text editor in the console, which will validate your schema.

This section will first cover the required definitions for the OpenAPI schema. The next section will cover best practices and examples for configuring OpenAPI schema definitions to maximize the accuracy of your Amazon Q Business custom plugins. For more details about OpenAPI schemas, see OpenAPI specification on the Swagger website.

Topics

- OpenAPI Schema definitions for custom plugins

OpenAPI Schema definitions for custom plugins

The following is the general format of an OpenAPI schema for a custom plugin.

```
{
    "openapi": "3.0.0",
    "servers": [
    {
```

```
      "url": "https://api.example.com"
    }
  ],
    "paths": {
        "/path": {
            "method": {
                "description": "string",
                "operationId": "string",
                "parameters": [ ... ],
                "requestBody": { ... },
                "responses": { ... },
                "security": [ ... ]
            }
       }
    },
    "security": [
        {
            "OAuth2": ["read", "write"]
        }
    ],
    "components": {
    "securitySchemes": {}
 }
}
```

The following list describes fields in the OpenAPI schema

- `openapi` – (Required) The version of OpenAPI that's being used. This value must be `"3.0.0"` or higher for custom plugins.
- `servers` – (Required) The identifier for application connectivity from API clients. This is required for the custom plugin call to succeed.
- `paths` – (Required) Contains relative paths to individual endpoints. Each path must begin with a forward slash (`/`). Amazon Q Business supports only one configured endpoint per custom plugin.
- `method` – (Required) Defines the method to use.
- `securitySchemes` – (Optional) Defines the OAuth security parameters.
- `security` – (Required when using authentication) Defines which security schemes are applied to the whole API or specific operations. This is required when using OAuth authentication.

Minimally, each method requires the following fields:

- `description` – A description of the API operation. Use this field to let the custom plugin know when to call this API operation and what the operation does.
- `responses` – Contains properties that the custom plugin returns in the API response. The custom plugin uses the response properties to construct prompts, accurately process the results of an API call, and determine a correct set of steps for performing an action.

The fields within the following two objects provide more information for your custom plugin to effectively select API operations that are needed to fulfill an end user request. For each field, set the value of the `required` field to `true` if required and to `false` if optional.

- `parameters` – Contains information about parameters that can be included in the request.
- `requestBody` – Contains the fields in the request body for the operation. Don't include this field for `GET` and `DELETE` methods.

For details on configuring the fields review the following sections:

Topics

- OpenAPI Schema responses
- OpenAPI Schema parameters
- OpenAPI Schema request body
- OpenAPI Schema security schemes

OpenAPI Schema responses

The following is a sample response.

```
"responses": {
    "200": {
        "content": {
            "<media type>": {
                "schema": {
                    "properties": {
                        "<property>": {
                            "type": "string",
                            "description": "string"
                        },
                        ...
```

```
                    }
                }
            }
        },
    },
    ...
}
```

Each key in the `responses` object is a response code, which describes the status of the response. The response code maps to an object that contains the following information for the response:

- `content` – (Required for each response) The content of the response.
- *`<media type>`* – The format of the response body. At this time, only `application/json` is supported by custom plugins. For more information, see Media types on the Swagger website.
- `schema` – (Required for each media type) Defines the data type of the response body and its fields.
- `properties` – (Required if there are `items` in the schema) Your custom plugins uses properties that you define in the schema to determine the information it needs to return to the end user in order to fulfill a task. Each property contains the following fields:
  - `type` – (Required for each property) The data type of the response field.
  - `description` – (Optional) Describes the property. The custom plugin can use this information to determine the information that it needs to return to the end user.

OpenAPI Schema parameters

The following are examples of parameters.

```
"parameters": [
    {
        "name": "string", // e.g. "userName"
        "description": "string",
        "required": boolean,
        "x-amzn-form-display-name": "string" // e.g. "User Name"
        "schema": {
            ...
        }
    },
    {
        "name": "string", // e.g. "employeeId"
```

```
        "description": "string",
        "required": boolean,
        "x-amzn-form-hide": boolean //e.g. true
        "schema": {
            ...
        }
    }
    ...
]
```

Your custom plugin uses the following fields to determine the information it must get from the end user to perform the plugin's requirements.

- `name` – (Required) The name of the parameter.
- `description` – (Required) A description of the parameter. Use this field to help the plugin to understand how to elicit this parameter from the user or determine that it already has that parameter value from prior actions or from the user's request to the custom plugin.
- `required` – (Optional) Whether the parameter is required for the API request. Use this field to indicate to the custom plugin whether this parameter is needed for every invocation or if it's optional.
- `schema` – (Optional) The definition of input and output data types. For more information, see Data Models (Schemas) on the Swagger website.
- Extension support – (Optional) For a write API operation, an Amazon Q Business custom plugin may dynamically create a confirmation form that is presented to end users. This form allows users to confirm and/or correct parameters Amazon Q populated based on the end user's request or past actions. The following extensions can be used to modify how that form is created:
  - `x-amzn-form-display-name` – (Optional) This can be used at parameter level to override the default name visible in the form.
  - `x-amzn-form-hide` – (Optional) This can be used to hide a parameter from being displayed in the user facing form.
- Schemas containing composition keywords (`allOf`, `not`, `oneOf`, or `anyOf`) are not supported.
- Schemas containing array types are not supported. For example, schemas such as `{"type": "array", "items": {"string"}}` are not supported.

OpenAPI Schema request body

The following is the general structure of a `requestBody` field:

```
"requestBody": {
    "required": boolean,
    "content": {
        "<media type>": {
            "schema": {
                "properties": {
                    "<property>": {
                        "type": "string",
                        "description": "string"
                    },
                    ...
                }
            }
        }
    }
}
```

The following list describes each field:

- `required` – (Optional) Whether the request body is required for the API request.
- `content` – (Required) The content of the request body.
- *`<media type>`* – (Optional) The format of the request body. At this time, only `application/json` is supported by custom plugins. For more information, see Media types on the Swagger website.
- `schema` – (Optional) Defines the data type of the request body and its fields.
- `properties` – (Optional) Your custom plugin uses properties that you define in the schema to determine the information it must get from the end user to make the API request. Each property contains the following fields:
  - `type` – (Optional) The data type of the request field.
  - `description` – (Optional) Describes the property. The custom plugin can use this information to determine the information it needs to return to the end user.
- Schemas containing composition keywords (`allOf`, `not`, `oneOf`, or `anyOf`) are not supported.
- Schemas containing array types are not supported. For example, schemas such as `{"type": "array", "items": {"string"}}` are not supported.

OpenAPI Schema security schemes

Following is the general structure of a `securityScheme` field:

```
"securitySchemes": {
      "OAuth2": {
        "type": "oauth2",
        "flows": {
          "authorizationCode": {
            "authorizationUrl": "https://example.com/oauth/authorize",
            "tokenUrl": "https://example.com/oauth/token",
            "scopes": {
              "read": "Read access to resources",
              "write": "Write access to resources"
            }
          }
        }
      }
    }
```

If your API requires OAuth authorization, the OpenAPI schema needs to include security schemes. We support the following authorization code flow of OAuth:

- `type` – Must be `oauth2`.
- `flows` – Must contain `authorizationCode`.
- `authorizationUrl` – The URL to which the user will be sent to begin the authorization process.
- `tokenUrl` – (Optional) The URL that the custom plugin will use to exchange the authorization code for an access token.
- `scopes` – Defines the permissions that the custom plugin will request.

Successful authorization using OAuth also requires an OAuth client ID, client secret, and a redirect url. These will need to be provided as secrets when creating the custom plugin.

Best practices for OpenAPI schema definition for custom plugins

While application programming interfaces (APIs) have traditionally been used by developers to integrate with external applications, today APIs are increasingly being used by generative AI-powered assistants, such as Amazon Q Business custom plugins. However, its important to note that APIs being used with AI assistants may require design optimizations that were not critical

for traditional application integrations. Following the best practices below will help Amazon Q Business to maximize the accuracy and improve efficiency when resolving end user requests.

Topics

- Optimizing OpenAPI schema accuracy
- Best practices for OpenAPI Schema names
- Best practices for OpenAPI Schema descriptions
- Best practices for JSON input schemas
- Other important considerations for OpenAPI specifications
- Example of API Schema optimization

Optimizing OpenAPI schema accuracy

To create a custom plugin, you need to create or edit an OpenAPI schema outlining the different API actions you want to enable for your custom plugin. Once the custom plugin is deployed, Amazon Q Business will process an end user prompt and use the OpenAPI schema to dynamically determine the appropriate APIs to call to accomplish the user's goal. Therefore, the OpenAPI schema definition has a big impact on API selection accuracy.

The following are the OpenAPI schema sections you need to optimize to maximize the accuracy of your Amazon Q Business plugins:

- **Names** – Names for operation IDs, parameters, object schema property keys, title in info section, and more.
- **Descriptions** – Descriptions for operations, parameters, schemas, and more.
- **JSON schemas** – JSON schemas for API inputs (schemas defined in parameters and request body). Within these schemas, important information includes the data type of each schema and format information (for example, date/date-time for ISO-8601 date strings), as well as names and descriptions mentioned above.

In the next sections, we outline how you can maximize the accuracy of your custom plugin by following best practices for your OpenAPI schema parameters.

Best practices for OpenAPI Schema names

- Names and IDs should be human-readable, descriptive, and unambiguous while being as concise as possible.
- Operation IDs provide important signals for understanding the function of each operation. Though not required, it is recommended to add `operationIds` to your API schema. The following outlines some Operation ID naming best practices:
  - Avoid noun-only `operationIds`, like `contacts`. Instead, prefix operation names with descriptive verbs like `get`, `find`, `search`, `create`, `update`, and `delete`. For example, `getContacts`.
  - Ensure `operationIds` meaningfully relate to the function of the operation. Avoid including `operationIds` with meaningless suffixes/prefixes, like `search_1` and `search_2`. If multiple operations perform similar functions, but differ only by inputs, consider creating IDs like `searchByName` or `searchByEmail`, or even merging these operations.
  - Avoid adding long, redundant prefixes to names. For example, avoid `contactsPlugin.getContacts` and `contactsPlugin.createContact`. Instead, use `getContacts` and `createContact`.
- Names of input request body properties and parameters are important for determining the role and purpose of each input needed for invoking an operation. The following outlines some input request naming best practices:
  - Avoid non-descriptive parameter names like `id`. Instead include a descriptive noun, like `contactId`.
  - It's not necessary to include information that is redundant with the JSON data type of the input. For example, avoid using `recipientEmailsArray` and instead just use `recipientEmails`.
- Be consistent with parameter names. Generally, parameters and response properties with the same name should mean the same thing across all operations in your schema. The following outlines some parameter naming best practices:
  - Avoid using different names for parameters with the same meaning. For example, `start_date` in one API and `begin_date` in another API if they mean the same thing.
  - Ensure parameter names and property names in responses are consistent with each other. For example, if an API returns `begin_date`, then also use the name `begin_date` in the input parameters if they have the same meaning.

Best practices for OpenAPI Schema descriptions

- Descriptions should be self-contained, providing sufficient guidance for how and when to use the operation or parameter they describe. The following outlines some description creation best practices:
  - Operation descriptions should describe what the operation does, including when, when not, and how to use it.
  - Avoid verbose descriptions. Parameter descriptions should concisely describe their purpose and how they impact the behavior of the operation. For example, rather than write “this field accepts an ISO-8601 date, which is of the format YYYY-MM-DD”, assign date to the format field.
  - Concise explanations are generally more useful than examples.
  - Make dependencies between operations explicit in the description. If an operation always requires another operation to be called first (such as, populating an input parameter from the other operation’s outputs), make this clear in the description of the operation or parameter.
- Use descriptions only where there is ambiguity or missing context. Avoid adding descriptions that provide no additional information. Restrict the description to information needed to use the API for the use cases Amazon Q Business custom plugin is intended to handle.
- Descriptions should not reference external links/URLs. Amazon Q Business custom plugins may not be able to access these.
- Avoid referencing operations by their *path* or *verb*. Instead use their operation ID when referring to other operations in descriptions.
- Avoid referencing schema components or API paths (except dependency `operationIds`) in the description. Ensure that descriptions are self-contained. As an exception to this, descriptions may reference dependency operations by their `operationIds` but should avoid providing specific usage examples of the operation. The following outlines some referencing best practices:
  - Don’t refer to operations by their API paths (e.g. `/api/v1/timeoff/requests`). Instead, use `operationIds` to refer to operations in descriptions. For example, `GetTimeOffRequests`.
  - Don’t refer to schema components like `#/components/schemas/TimeOffRequest`.
  - If examples are necessary, describe them in abstract terms. “For example, use `{operationId}` to do `{X}`” or “Use `{operationId}` when the end user asks for...”.
  - Internally, Amazon Q Business may use generate API calls differently than described in the OpenAPI schema. So, including usage examples may not always be helpful.

Best practices for JSON input schemas

- Simpler interfaces will lead to more efficient, consistent, and accurate plugin usage from Amazon Q Business. Thus, having fewer input parameters of lower complexity is best.
- Keep the total number of parameter schemas per operation low. Keeping the total number of parameter schemas to 10 at most, but less than 4 on average, will give the best results. Having more parameters may result in slower responses because Amazon Q Business custom plugins will need to fill out each field.
- Avoid including unnecessary optional input parameters. For example, for search APIs with many parameters for filtering results, use the most informative/important filters. Or, split into multiple operations to search by alternate criteria.
- Avoid structurally complex/nested inputs when possible. The following outlines some input parameter structure best practices:
  - **Instead of** `{"start": {"type": "object", "properties": {"date": {...}, "time": {...}}, "end": {...}}` **input** `{"start_date": {...}, "start_time": {...}, ..., "end_time": {...}}`.
  - Avoid schemas containing array types, which are not supported. For example, schemas such as `{"type": "array", "items": {"string"}}` are not supported..
  - Avoid circular references (`$ref` inside of `$ref`). Circular references can occur in nested structures when the same reference (`$ref`) appears inside of its de-referenced value. Although these are valid OpenAPI specifications, Amazon Q Business custom plugin may not reliably resolve these recursive definitions.
  - Avoid composition keywords (`allOf`, `not`, `oneOf`, or `anyOf`), which are not supported
- Use standard values in the format field for string parameters. For example, `date-time` or `date` for capturing ISO-8601 dates/times.

Other important considerations for OpenAPI specifications

- Never expose sensitive information in the API schema or API outputs. If information should not be exposed to the end user, do not include it in your API specification or use an API that produces such outputs.
- If it is undesirable for an Amazon Q Business custom plugin to reference certain information in the API schemas to the end user, you can use instructions in the operation descriptions to help discourage this. However, you should not rely on this mechanism for highly sensitive information.

- Only include essential information in API responses. Redundant or excessively verbose information will reduce the efficiency of an Amazon Q Business custom plugin.
- Limit paginated search results explicitly, particularly if each result returned is large/complex. Large API responses may result in slower responses for end users. Consider setting guidance or limits in the description of the parameter (for example, set to five at most).
- Only 2XX responses may be shared with Amazon Q Business custom plugin end users. 4xx and 5xx responses will not be shared with end users. If you want to expose specific errors from the API, consider using a 2XX code for such errors. Ensure you include information that is appropriate to share with the end user.
- The OpenAPI specification should be self-contained. Ensure that the set of API operations described in the schema support complete use cases without relying on APIs not defined or other plugins.

Example of API Schema optimization

This section shows you an example of an API schema before and after our best practices are applied. The example API is used for managing Paid Time Off (PTO) requests for employees and supports two operations: checking the status of requests (with `api.V1.TimeOffRequest`) and making new requests (with `api.V1.RequestTimeOff`).

The following is the example unoptimized API Schema:

```
openapi: 3.0.3
info:
  # title is too long
  title: API for PTO Request Management
  version: 1.0.0
servers:
  - url: https://api.example.com
paths:
  /api/v1/timeoff/requests:
    get:
      # operation ID is ambiguous (is it to get a time off request or make one?) and
 contains unnecessary details ("api.V1")
      operationId: example.api.V1.TimeOffRequest
      # description is not self-contained (references an external link) and does not
 describe what the API returns or how to use it.
      description: Existing requests for the authenticated user. See the docs <a
 href=https://example.com>here</a> for more details.
```

```
      parameters:
        - name: type
          in: path
          # description does not include what a "type" is
          description: type to filter by
          required: false
          schema:
            type: string
        - name: status
          in: path
          # description does not include what a "status" is
          description: status to filter by
          required: false
          schema:
            type: string
        - name: start
          in: path
          # description is ambiguous
          description: start of range to include
          required: false
          schema:
            type: string
            # no formatting information is provided, e.g. `format: date`
        - name: end
          in: path
          # description is ambiguous
          description: end of range to include
          required: false
          schema:
            type: string
            # no formatting information is provided, e.g. `format: date`
        - name: limit
          in: path
          # guidance should be provided on how many results to return by default, e.g.
 less than 5
          description: limit on the number of requests to return
          required: false
          schema:
            type: integer
        - name: page
          in: path
          description: specific page of results to return if results are paginated
          required: false
          schema:
```

```
            type: integer
      responses:
        "200":
          description: OK
          content:
            application/json:
              schema:
                $ref: "#/components/schemas/TimeOffRequests"
  /api/v1/timeoff/request:
    post:
      # operation ID is ambiguous (is it to get a time off request or make one?) and
 contains unnecessary details ("api.V1")
      operationId: example.api.V1.RequestTimeOff
      # description is not self-contained (references an external link) and ambiguous.
      description: Make a request for the authenticated user. <a href=https://
example.com/>API docs</a> for more details.-->
      requestBody:
        content:
          application/json:
            schema:
              type: object
              properties:
                # this field adds unnecessary nesting to the inputs. Separate
 `start_date`, and `end_date` fields would be preferred
                range:
                  # missing a description, non-descriptive field name
                  type: object
                  properties:
                    start:
                      # start of what?
                      type: string
                      format: date
                    end:
                      # end of what?
                      type: string
                      format: dat
                  required:
                    - start
                    - end
                type:
                  description: the type of request to make, e.g. `Personal` or
 `Vacation`
                  type: string
                  # use enums where possible
```

```
                note:
                  description: a short note describing the reason for the request
                  type: string
      responses:
        "201":
          description: OK
          content:
            application/json:
              schema:
                $ref: "#/components/schemas/TimeOffRequest"
components:
  schemas:
    TimeOffRequest:
      type: object
      properties:
        # this ID is not necessary for the end user (and is used nowhere else in the
 API), consider removing
        id:
          type: string
        status:
          # no descriptions provided
          type: string
        type:
          type: string
        start:
          type: string
        end:
          type: string
        note:
          type: string
        duration:
          type: integer
        # this ID is not necessary for the end user (and is used nowhere else in the
 API), consider removing
        approver_id:
          type: string
        approver_display_name:
          type: string
    TimeOffRequests:
      type: array
      items:
        $ref: "#/components/schemas/TimeOffRequest"
```

Applying the best practices defined above, there are multiple updates that should be made to this API schema to get the best results when using Amazon Q Business custom plugins.

First, based on guidance to make names concise, descriptive and unambiguous, we'll make a few updates to the operation IDs, parameter names, and schema title:

- Change `example.api.V1.RequestTimeOff` to `CreateTimeOffRequest`
- Change `example.api.V1.RequestTimeOff` to `GetTimeOffRequests`
- Change the schema title in the info section from `API for PTO Request Management` to `TimeOff`

If you are able to change the API itself, we'd also like you to fix parameter names. Change parameters named `type` and `status` to `request_type` and `request_status` respectively

Next, based on best practices for descriptions, we'll make the following updates:

- Modify the description of `/api/v1/timeoff/requests` and `/api/v1/timeoff/request` to make them self-contained (remove URL) and describe what they do and how to use them. For example:
  - Change `Existing requests for the authenticated user. See the docs <a href=https://example.com>here</a> for more details.` to `Return existing time off requests (including information like the current approval status, dates/days used) for the authenticated user.`
  - Change `Make a request for the authenticated user. See <a href=https://example.com/>API docs</a> for more details.` to `Create a new time off request of a particular type (e.g. Personal or Vacation) for the authenticated user based on a start and end date (inclusive).`
- Add descriptions for ambiguous parameters. For example:
  - For the end date of a request, add a description: `Last day for the request (inclusive) in ISO-8601 format (for example, YYYY-MM-DD).`
  - For the start date, add a description: `First day of the request in ISO-8601 format (e.g. YYYY-MM-DD).`
- Based on guidance to limit paginated search results explicitly, we'll add a description to the `limit` field in `GetTimeOffRequests`. For example, `Limit on the number of requests to return. Limit to 5 unless otherwise instructed.`

Finally, we'll apply changes based on the API input schema best practices:

- Assuming we have control over the API implementation, we'd like to apply guidance on avoiding unnecessary nesting. For this, we can convert `range` (which contains start and end dates) to two top-level properties called `startDate` and `endDate`.
- Following guidance to use standard format fields, we'll add format: `date` to start/end date fields (assuming we are expecting standard date formats).

After making corrections, we end up with a vastly improved API specification that will maximize the Amazon Q Business custom plugin accuracy and efficiency in resolving user requests.

The following is the API Schema after we've added optimization fixes:

```
openapi: 3.0.3
info:
  title: TimeOff
  version: 1.0.0
servers:
  - url: https://api.example.com
paths:
  /api/v1/timeoff/requests:
    get:
      operationId: GetTimeOffRequests
      description: Return existing time off requests (including information like the
 current approval status, dates/days used) for the authenticated user
      parameters:
        - name: request_type
          in: path
          required: false
          schema:
            type: string
            enum:
              - Vacation
              - Personal
              - JuryDuty
              - Sick
        - name: request_status
          in: path
          required: false
          schema:
            type: string
            enum:
```

```
              - Approved
              - Pending
              - Cancelled
        - name: start
          in: path
          description: Include requests ending on or after this date
          required: false
          schema:
            type: string
            format: date
        - name: end
          in: path
          description: Include requests starting before this date
          required: false
          schema:
            type: string
            format: date
        - name: limit
          in: path
          description: Limit on the number of requests to return. Limit to 5 unless
otherwise instructed
          schema:
            type: integer
        - name: page
          in: path
          description: Specific page of results to return if results are paginated
          required: false
          schema:
            type: integer
      responses:
        "200":
          description: OK
          content:
            application/json:
              schema:
                $ref: "#/components/schemas/TimeOffRequests"
 /api/v1/timeoff/request:
   post:
     operationId: CreateTimeOffRequest
     description: Create a new time off request for the authenticated user
     requestBody:
       content:
         application/json:
           schema:
```

```
              type: object
              properties:
                startDate:
                  description: First day of the request in ISO-8601 format (e.g. YYYY-
MM-DD)
                  type: string
                  format: date
                endDate:
                  description: Last day for the request (inclusive) in ISO-8601 format
 (e.g. YYYY-MM-DD)
                  type: string
                  format: date
                request_type:
                  description: The type of request to make, either `Personal`,
 `Vacation`, `Sick` or `JuryDuty`
                  type: string
                  enum:
                    - Personal
                    - Vacation
                    - Sick
                    - JuryDuty
                note:
                  description: A short (one to two sentence) note describing the reason
 for the request
                  type: string
              required:
                - startDate
                - endDate
                - request_type
                - note
      responses:
        "201":
          description: OK
          content:
            application/json:
              schema:
                $ref: "#/components/schemas/TimeOffRequest"
components:
  schemas:
    TimeOffRequest:
      type: object
      properties:
        # this ID is not necessary for the end user (and is used nowhere else in the
 API), consider removing
```

```
        request_id:
          type: string
        request_status:
          description: the current status of the request, either `Pending`, `Approved`,
or `Cancelled`
          type: string
          enum:
            - Pending
            - Approved
            - Cancelled
        request_type:
          type: string
        start:
          description: the start date of the request
          type: string
        end:
          description: the last date of the request (inclusive)
          type: string
        note:
          description: brief note describing the reason for the request
          type: string
        duration:
          description: the number of working days used for the request
          type: integer
        approver_display_name:
          description: the name of the person of who approved the request
          type: string
    TimeOffRequests:
      type: array
      items:
        $ref: "#/components/schemas/TimeOffRequest"
```

Creating an Amazon Q Business custom plugin

Note

To validate accuracy before deploying to end users, we recommend creating a Amazon Q Business test application to configure and test new features. To create a new custom plugin, first ensure that you have a test application with the same settings and configurations as your production application (the one deployed for your end users). Using the console, configure a custom plugin in the test application following the steps below. After you finish configuring your custom plugin, launch a test web experience and login

as an end user. Issue a number of expected user prompts and confirm you are getting the expected results. If you are not getting the expected results, return to the console page and modify the OpenAPI specification to ensure it follows best practices for configuring OpenAPI specifications. Repeat this process until you are satisfied with the test application results and then replicate the same custom plugins settings in your production application before you share it with your end users.

You use the `CreatePlugin` action to create an Amazon Q custom plugin for your web experience chat. The following tabs provide a procedure for the AWS Management Console and code examples for the AWS CLI.

To create a custom plugin, choose a tab based on your access preference for Amazon Q.

Console

To create a application-name plugin

1. Sign in to the AWS Management Console and open the Amazon Q Business console.
2. From the Amazon Q Business console, in **Applications**, click on the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. In **Plugins**, choose **Add plugin**.
5. In **Add plugins**, choose **Custom plugin**.
6. In **Custom plugin**, enter the following information:

    a. In **Name and description**, for **Plugin name** – A name for your Amazon Q plugin. The name can include hyphens (-) but not spaces and can have a maximum of 1000 alphanumeric characters.

    b. In **API schema**, for **API schema source**, choose from the following options:

    - **Select from Amazon S3** – Choose this to select an existing API schema from an Amazon S3 bucket. Your API schema must have an API description, structure, and parameters for your custom plugin. Then, enter the **Amazon S3 URL** to your API schema.

- **Define with in-line OpenAPI schema editor** – Choose this to write your custom plugin API schema in the inline OpenAPI schema editor in the Amazon Q console. A sample schema appears that you can edit. Then, you can choose to do the following:
  - Select the format for the schema, whether **JSON** or **YAML**.
  - To import an existing schema from S3 to edit, select **Import schema**, provide the S3 URL, and select **Import**.
  - To restore the schema to the original sample schema, select **Reset** and then confirm the message that appears by selecting **Reset** again.

c. **Authentication** – Choose between **Authentication required** or **No authentication required**. If no authentication is required, there is no further action needed. If authentication is required, choose to **Create and add a new secret** or **Use an existing one**. Your secret must contain:

i. **Secret name** – A name for your Secrets Manager secret.

ii. **Client ID** – The client ID you copied from your third-party application.

iii. **Client secret** – The client secret you copied from your third-party application.

iv. **OAuth callback URL** – The URL to which user needs to be redirected after authentication. If your deployed web url is `<q-endpoint>`, use `<q-endpoint>/oauth/callback` . Amazon Q Business will handle OAuth tokens in this URL. This callback URL needs to be allowlisted in your third-party application.

v. In **Choose a method to authorize Amazon Q Business** – Choose to **Create and add a new service role** or **Use an existing service role**. Make sure your service role has the necessary permissions.

The console will generate a **Service role name**.

7. **Tags – *optional*** – An optional tag to track your plugin.
8. Select **Add plugin** to add your plugin.

CLI

To create a custom plugin

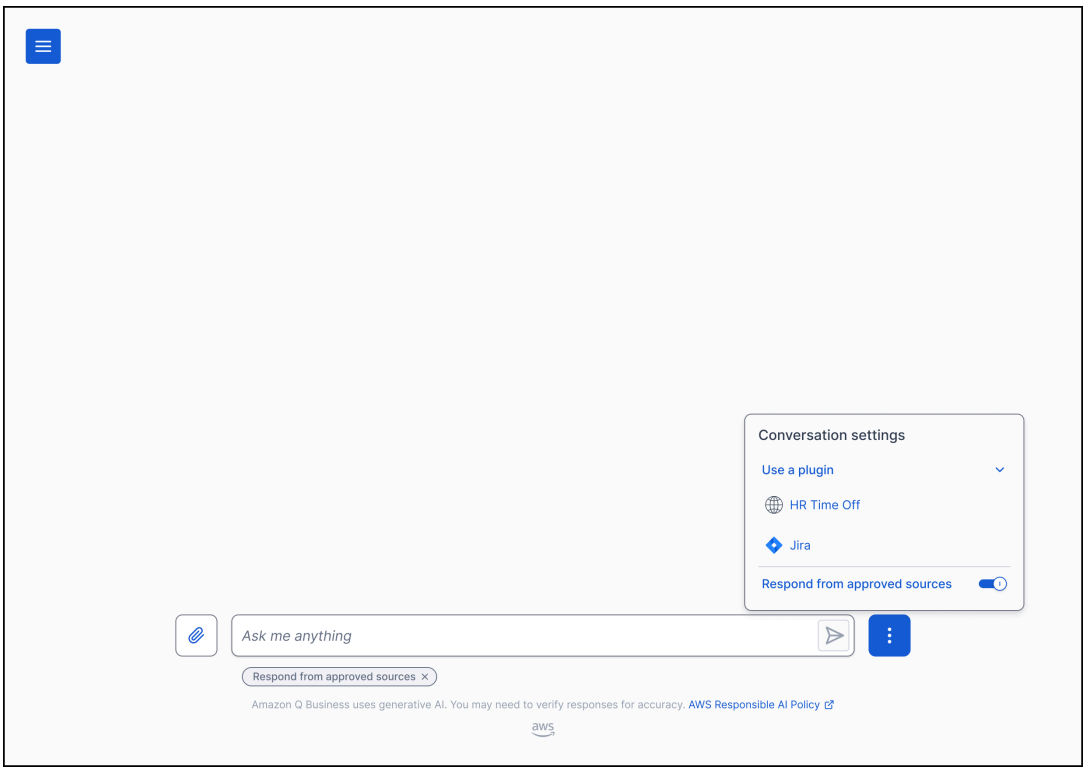
```
aws qbusiness create-plugin \
--application-id application-id \
--display-name display-name \
```

```
--type CUSTOM \
--auth-configuration basicAuthConfiguration="'{"noAuthConfiguration": {}}' \
--custom-plugin-configuration '{"description":"description, "apiSchemaType":
 "OPEN_API_V3", "apiSchema": {"s3": {"bucket": s3_bucket_with_openapi_schema
 "key":s3_key_with_openapi_schema}}}'"
```

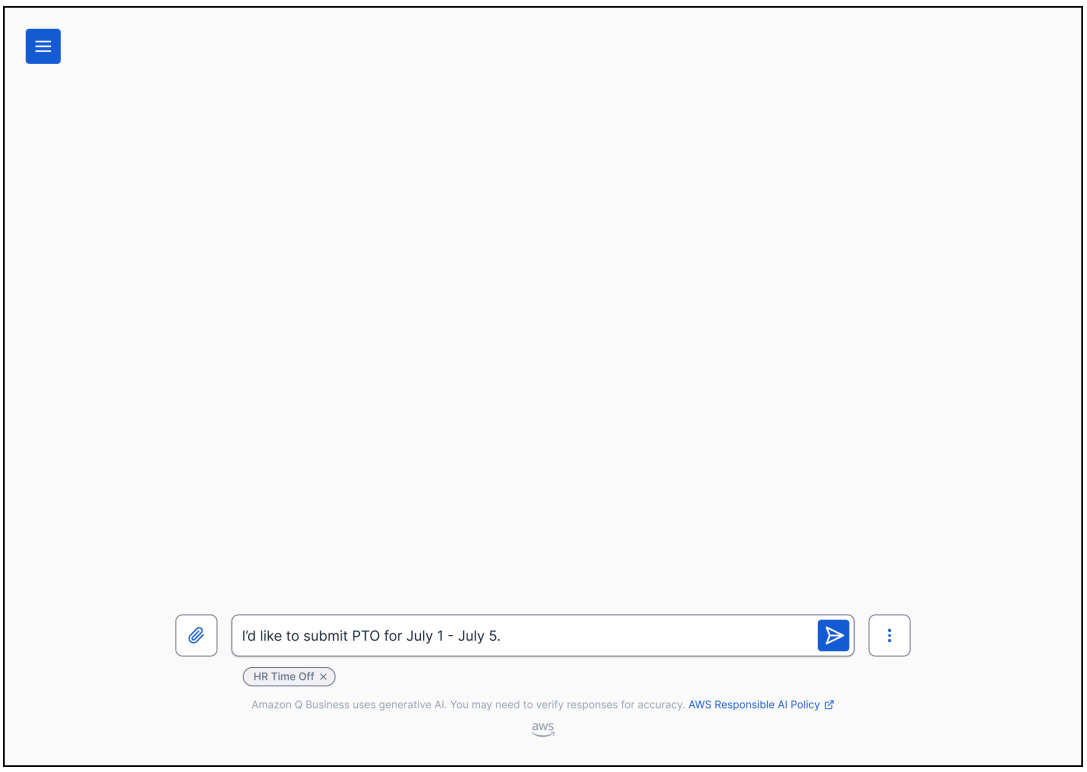
Using an Amazon Q Business custom plugin

Once a custom plugin is deployed, end users can launch it from the menu icon in the Amazon Q Business web experience.

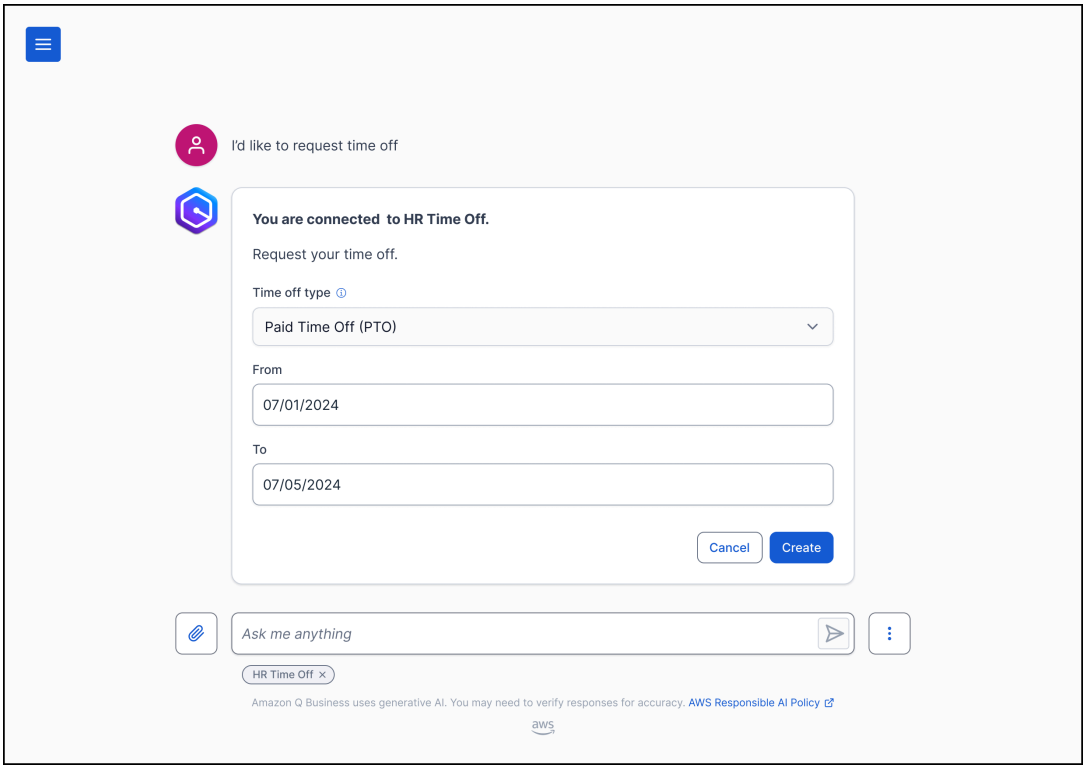
> **Note**
>
> If your Admin controls and guardrails settings allow Amazon Q to automatically orchestrate end user chat queries across plugins and data sources, plugin actions will be automatically activated by Amazon Q for your end user during chat. In that case, your end user won't have to follow the steps below.



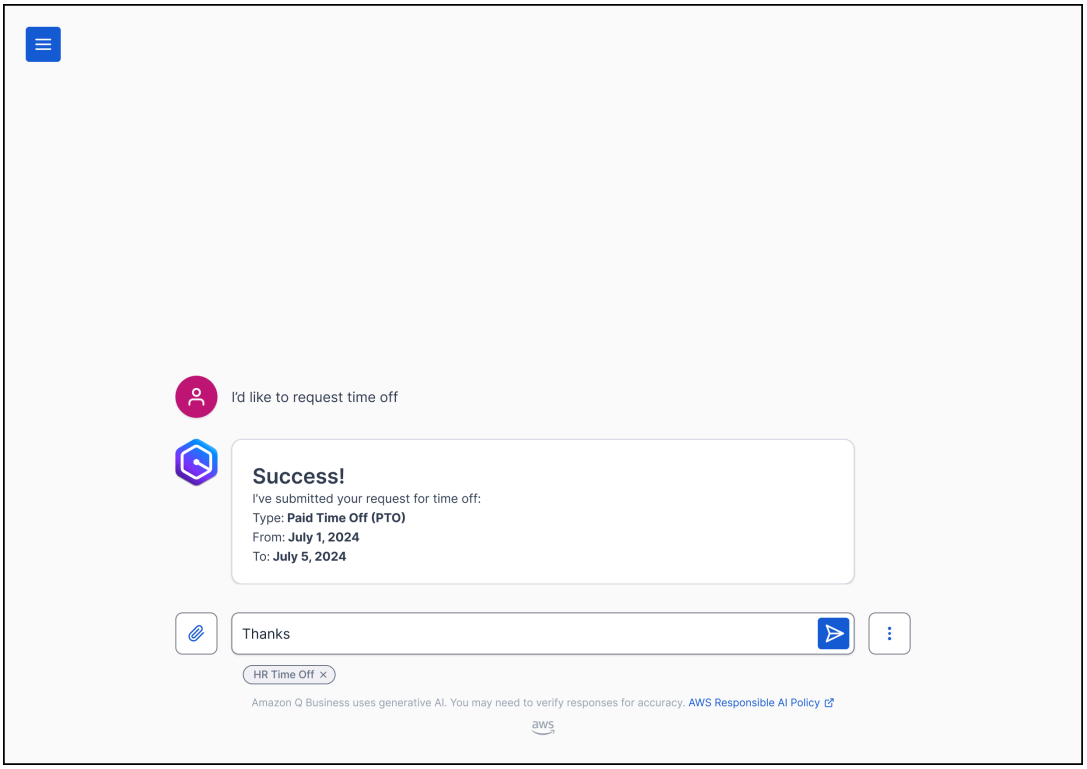
End users can then type a prompt.



If it is the first time an end user is accessing the custom plugin or their past login has expired, they will need to authenticate. After authenticating successfully, Amazon Q Business will perform the requested task. For a write API operation, end users will always get a confirmation form that allows them to confirm or correct parameters that were populated based on the request or past actions.



Once the user confirms the action, Amazon Q Business will submit the request and give the user confirmation once it is complete.



Managing Amazon Q Business plugins

To manage Amazon Q plugins, you can take the following actions:

Actions

- Updating a plugin
- Deleting a plugin
- Getting plugin properties
- Listing plugins
- Listing configured plugin actions
- Listing available plugin actions
- Listing plugin metadata

Updating a plugin

To update a plugin, you can use AWS Management Console or the UpdatePlugin API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To update a plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, select the plugin that you want to update, and then choose **Actions**.
5. For **Actions**, choose **Edit**.

   On the plugins configuration page, you can edit your settings.

To deactivate a plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.

3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, select the plugin that you want to deactivate, and then choose **Actions**.
5. For **Actions**, choose **Deactivate**.

   Your plugin will be deactivated. After your plugin is deactivated, its status will change to **Inactive**.

To reactivate a plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, select the plugin that you want to reactivate, and then choose **Actions**.
5. For **Actions**, choose **Reactivate**.

   Your plugin will be activated. After your plugin is reactivated, its status will change to **Active**.

AWS CLI

To edit a plugin

```
aws qbusiness update-plugin \
--application-id application-id \
--plugin-id plugin-id \
--display-name display-name \
--server-url https://example.atlassian.net \
--auth-configuration basicAuthConfiguration="{secretArn=<secret-arn>,roleArn=<role-arn>}"
```

To disable a plugin

```
aws qbusiness update-plugin \
--application-id application-id \
--plugin-id plugin-id \
```

```
--state DISABLED
```

To enable a plugin

```
aws qbusiness update-plugin \
--application-id application-id \
--plugin-id plugin-id \
--state ENABLED
```

Deleting a plugin

To delete a plugin, you can use the AWS Management Console or the DeletePlugin API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To delete a plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, select the plugin that you want to delete, and then choose **Actions**.
5. For **Actions**, choose **Delete**.
6. In the dialog box, type **`delete`** to confirm your action.

   The console displays a successful deletion message when the plugin deletion process is finished.

AWS CLI

To delete a plugin

```
aws qbusiness delete-plugin \
--application-id application-id \
--plugin-id plugin-id
```

Getting plugin properties

To get the details of an Amazon Q plugin, you can use either the AWS Management Console or the GetPlugin API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To get plugin details

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. For **Plugins**, select the configured plugin that you want to see details for.
5. On the **Plugin settings** page, the following details are available:

   - **Name** – The name of your plugin.
   - **Type** – The type of your plugin.
   - **AWS Secrets Manager** – The Secrets Manager secret.
   - **Creation time** – The time stamp for when your plugin was created.
   - **Plugin ID** – The ID that's assigned to your plugin.

AWS CLI

To get plugin details

```
aws qbusiness get-plugin \
--application-id application-id \
--plugin-id plugin-id
```

Listing plugins

To list Amazon Q plugins, you can use the AWS Management Console or the ListPlugins API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To list plugins

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. In **Plugins**, a list of plugins that are attached to your application is available.

AWS CLI

To list plugins

```
aws qbusiness list-plugins \
--application-id application-id
```

Listing configured plugin actions

To list actions configured for a specific Amazon Q plugin, you can use the AWS Management Console or the ListPluginActions API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To list specific actions configured for a plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. In **Plugins**, select your plugin from the list of plugins configured for your application.
5. On the plugin summary page, you'll find the actions supported by your plugin under **Actions supported**.

AWS CLI

To list specific actions configured for a plugin

```
aws qbusiness list-plugin-actions \
--application-id application-id \
--plugin-id plugin-id
```

Listing available plugin actions

To list all available actions for a specific Amazon Q plugin, you can use the AWS Management Console or the ListPluginTypeActions API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To list all available actions for a specific plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. On the **Plugins** page, under each plugin type, you'll find all the plugins actions supported by Amazon Q Business.

AWS CLI

To list all available actions for a specific plugin

```
aws qbusiness list-plugin-type-actions \
--plugin-type SERVICE_NOW | SALESFORCE | JIRA | ZENDESK | CUSTOM | QUICKSIGHT
 | SERVICENOW_NOW_PLATFORM | JIRA_CLOUD | SALESFORCE_CRM | ZENDESK_SUITE |
 ATLASSIAN_CONFLUENCE | GOOGLE_CALENDAR | MICROSOFT_TEAMS | MICROSOFT_EXCHANGE |
 PAGERDUTY_ADVANCE | SMARTSHEET | ASANA
```

Listing plugin metadata

To list metadata for a specific Amazon Q plugin, you can use the AWS Management Console or the ListPluginTypeMetadata API operation. The following tabs provide a procedure for the console and code examples for the AWS CLI.

Console

To list metadata for a specific plugin

1. Sign in to the AWS Management Console and open the Amazon Q console.
2. From the Amazon Q console, in **Applications**, select the name of your application from the list of applications.
3. From the left navigation menu, choose **Actions**, and then choose **Plugins**.
4. On the **Plugins** page, under each plugin type, you'll find all the plugin metadata (category, description, and type) supported by Amazon Q Business.

AWS CLI

To list metadata for a specific plugin

```
aws qbusiness list-plugin-type-metadata
```

Amazon Q Business features

> **Note**
>
> Not all features in Amazon Q Business Pro are available in Amazon Q Business Lite. For information about what's included in Amazon Q Business Lite and what's included in Amazon Q Business Pro, see Amazon Q Business tiers. You must use the Amazon Q Business console to assign subscription tiers to your users.

In addition to enhancements, Amazon Q Business offers the following features:

- **Filtering using metadata** – Use document attributes to customize and control the end user chat experience. Currently supported for use with the Amazon Q Business API.
- **Source attribution with citations** – Verify responses using Amazon Q Business source attributions.
- **Upload files to a chat** – Let end users upload files directly to a chat and use uploaded file data to perform web experience tasks.
- **Personalizing chat responses** – Allow Amazon Q Business to customize chat responses to your end users by using the metadata that's associated with them—specifically, address and job related information—in your IAM Identity Center instance.
- **Quick prompts** – Feature sample prompts to inform end users about the capabilities of their Amazon Q Business web experience.
- **Hallucination mitigation** – Reduce Amazon Q Business chat hallucinations and improve response accuracy.
- **Agentic RAG** – Enhances Amazon Q Business standard retrieval augmented generation (RAG) capabilities with agentic workflows.

Topics

- Filtering chat responses using document attributes and metadata
- Source attribution with citations in Amazon Q Business
- Upload files to a chat in Amazon Q Business
- Personalizing Amazon Q Business chat responses

- Quick prompts in Amazon Q Business
- Hallucination mitigation in Amazon Q Business
- Agentic Retrieval Augmented Generation (RAG) in Amazon Q Business

Filtering chat responses using document attributes and metadata

> **Note**
>
> This section assumes that you have an understanding of document attributes and how they work in Amazon Q.

The Amazon Q Business API includes a feature that lets you filter by document attribute. By using this feature, you can customize and control chat responses for your end user using attributes—or metadata—attached to documents that are mapped to index fields. For example, if `data source type` is an attribute that's attached to your documents, you can specify that chat responses should be generated only from a specific data source.

Or, you can allow end users to restrict the scope of chat responses using the attribute filters that you have selected. For example, an end user can choose to have their chat responses generated using only documents from data sources that they specify.

Filtering chat responses using metadata has the following key benefits:

- **Q&A on LLM knowledge** – Users can ask questions and get answers from the general knowledge that the LLM has.
- **Ensure response relevance and accuracy** – You can indicate that responses should only be generated from specific authoritative sources within your data.
- **Control response context** – You can specify the file type (for example, PDF) and library or collection of documents (for example, business requirements documents) that responses are generated from.
- **Maintain response freshness** – You can restrict chat responses to come from only documents that were generated after a specific date.
- **Scope chat responses** – You can help your end users to narrow the scope of their responses and get to the right answer more quickly.

Amazon Q Business offers a set of reserved document attributes that you can use. You can also create custom document attributes that better represent your organization's data and use cases for more finely-tuned chat response control.

> **Important**
>
> Filtering using document attributes in chat is only supported using the API. Boosting search results using document attributes is supported using the console or the API.

Source attribution with citations in Amazon Q Business

The Amazon Q Business web experience chat response provides in-text source citations for responses that use the organization's data sources and knowledge base as a source. The chat response also provides a full list of the sources used to generate the response.

Amazon Q Business supports source attribution with citations. If you specify the `_source_uri` metadata field when you add metadata to your Amazon S3 bucket, the source attribution links returned by Amazon Q Business in the chat results will direct users to the configured URL. If you don't specify a `_source_uri`, users can still access the source documents through clickable citation links that will download the file at query time. This allows users to verify information even when no source URI is configured. To learn how to add metadata for your Amazon S3 connector, see Adding document metadata in Amazon S3.

In-text source citations

In-text citations are provided in the form of a numbered list at the end of a sentence. To view an in-text source citation, choose a citation number. Each citation provides the following attributes:

- **Title** – The title of the source document.
- **URL** – A linked URL that you can follow to view the source document.
- **Snippet** – The snippet from the document from the source document that was used to generate each sentence in the response.

Source list

Sources used to generate the response are provided at the end of the response. Each source listed provides the following attributes:

- **Citation number** – The number provided at the end of the sentences in the response.
- **Title** – The title of the document that's the source for the generated response.
- **Text segment** – A text extract from a source document that's used for source attribution.
- **URL** – The URL of the document that's the source for the generated response.

Upload files to a chat in Amazon Q Business

Users using the Amazon Q Business web experience can upload documents and use the uploaded documents to ask questions and summarize or analyze data based on the content of the uploaded documents. Amazon Q provides a list of recent documents, enabling users to find and reuse recently attached files in new conversations without re-uploading. Users can upload new files from their computer, select from recent files, or drag and drop files directly into any conversation.

Users can upload up to 20 files during a conversation. The maximum upload size for each file is 50 MB and 3.75 MB for images. The total parsed content for all files combined has to be under 665,000 characters. Documents uploaded through the chat interface are deleted with the associated conversation after 30 days of inactivity. Once files are attached to a conversation, they cannot be deleted individually. Users must delete the entire conversation to remove attached files.

Using the Amazon Q Business web experience, you can upload documents and use them to ask questions and summarize or analyze data based on their content. When you start a new conversation, you can upload new files, choose from a saved list of recent documents, or drag and drop files directly into the conversation.

To use this feature, enable **Allow end users to send queries directly to the LLM** in **Admin controls and guardrails**. For more information, see the Response settings topic in Admin controls and guardrails.

Amazon Q Business supports specific document types for upload. To learn more about the document types that can be uploaded, see Supported document formats in Amazon Q Business.

If you plan to upload comma separated value (CSV) or Microsoft Excel (XLS, XLSX) files, we recommend using tables that have no more than 4 columns and 10 rows for best results.

> **Important**
>
> Audio formats such as MP3, MP4, FLAC, WAV and Video formats such as MP4 and MOV are not supported for chat upload.

Personalizing Amazon Q Business chat responses

Amazon Q Business uses location and job-related information from your IAM Identity Center instance to generate personalized responses that are relevant to your end user. For example, if your end user asks "What are the company holidays for this year?", Amazon Q Business might list region-specific holidays based on their country.

To enable response personalization, add **Address** information and **Job related information** for users in the IAM Identity Center instance that connects to your Amazon Q Business application. For more information, see Add users in the IAM Identity Center User Guide.

User personalization data that's in your IAM Identity Center instance is connected to your Amazon Q Business application environment, and responses are personalized by default. You can deactivate response personalization at any time by using the Admin controls and guardrails feature in Amazon Q Business.

Quick prompts in Amazon Q Business

The Amazon Q Business web experience welcome page provides sample prompts to help your end users understand the types of questions and tasks that they can ask. Sample prompts are not enabled by default.

If you're an AWS Management Console customer who needs to configure the web experience for your end users, you can enable the sample prompts feature when you preview the web experience. For more information, see Customizing a web experience (IAM Identity Center) or Customizing a web experience (IAM).

> **Important**
>
> Before you enable sample prompts, make sure that the **Only produce responses from retrieval augmented generation (RAG)** check box for **Application guardrails** is not selected. For more information, see Customizing global controls.
> You can't create your own prompts or edit the provided sample prompts.

Hallucination mitigation in Amazon Q Business

A hallucination, in the machine learning context, is a confident response by an AI (artificial intelligence) application environment that isn't supported by its underlying data. Amazon

Q Business includes a hallucination prevention system that works in real-time during chat conversations.

The *hallucination mitigation* feature helps ensure more accurate retrieval augmented generation (RAG) responses from data connected to the application—either through connected data sources, or files uploaded during chat (up to 100,000 characters). During chat, Amazon Q Business evaluates a response for hallucinations. If a hallucination is detected with high confidence, it corrects the inconsistencies in its response real-time during chat and generates a new, edited message.

To activate hallucination mitigation, use Amazon Q Business admin controls and guardrails.

Hallucination mitigation isn't supported for the following use cases:

- Applications where chat orchestration is enabled.
- Plugin workflows.
- Responses generated from tabular data, or from transcripts of images, audio and video. Hallucination mitigation applies only to responses generated from textual data.

> **Important**
>
> Activating hallucination mitigation will increase chat response latency.

Agentic Retrieval Augmented Generation (RAG) in Amazon Q Business

Agentic RAG enhances the standard RAG workflow of Amazon Q Business with agentic retrieval and response capabilities. Unlike standard RAG's document retrieval and simple response generation process, Agentic RAG uses multiple intelligent agents and specialized data retrieval tools to deliver more comprehensive and accurate responses while maintaining conversation context.

With Agentic RAG system processes queries through a combination of the following coordinated steps:

- Analyzes both the user's question and conversation history and determines which retrieval tools to use
- Intelligently deconstructs complex queries into simpler ones

- Intelligently triggers multiple data retrieval tools as needed
- Provides disambiguating questions based on enterprise data to clarify user intent
- Synthesizes information from various sources, and generates responses with its underlying large language model
- Provides follow-up questions to intelligently continue the conversation

Throughout this process, it continuously checks response quality and activates additional data retrieval tools when necessary, showing users real-time progress to the user as it processes queries. All responses maintain existing permissions and include clear citations to source material.

Agentic RAG delivers several key improvements over standard RAG. It intelligently selects from available retrieval tools based on query requirements and performs multiple retrieval operations for complex queries. The system maintains conversation context awareness and adapts response generation through retries or disambiguation techniques based on the quality of retrieved information and the subsequent response generated. These capabilities result in higher accuracy, more comprehensive information gathering, and better handling of complex, multi-faceted queries.

To use Agentic RAG, enable the feature using the **Advanced search** toggle in your web experience interface.

> **Note**
>
> While the Agentic RAG system provides more thorough responses, response times may be longer than standard RAG due to its multiple retrieval operations.

Using an Amazon Q Business web experience

You can use the Amazon Q Business web experience generative AI assistant to ask questions and to accomplish your tasks. When you ask a question, the Amazon Q Business web experience analyzes the latest approved data collected from data sources within your organization to generate a comprehensive response.

You can ask complex questions in plain language and get a detailed response. You can also use an Amazon Q Business web experience to perform tasks for you, such as draft an email message or create a Jira ticket.

> **Note**
>
> As of Oct 31, 2024, once you have created a new Amazon Q Business application environment, the default web experience will allow users to interact directly with the LLM to get answers from its general knowledge or uploaded file content, even if the Admin has not yet connected any enterprise data sources.
> For existing application environments, the *Allow direct access to LLM* setting will remain as previously configured. For new application environments, the *Allow direct access to LLM* setting will be enabled by default, though Admins can still disable this if desired.

The Amazon Q Business web experience provides you with the following capabilities:

Web experience features

- Example prompts
- Engage with contextual responses
- Analysis and reasoning
- Perform actions using plugins
- Review source citations
- Upload files and chat
- Advanced search
- Copy responses
- Provide feedback
- Conversation management

- Response sources
- Login, Logout and session duration for Web Experience

> **Important**
>
> An Amazon Q Business web experience establishes a secure WebSockets connection to supported Amazon Q Business endpoints over port 8443. For example, `wss://qbusiness.us-west-2.api.aws:8443/chat`.
> To ensure that your browser can successfully establish a WebSockets connection, ensure that port 8443 is enabled and not blocked by network rules that you have configured at the router, VPN, VPC, or firewall level.

Example prompts

The welcome page optionally provides example prompts to help you understand the types of questions and tasks that you can ask the Amazon Q Business web experience. This feature is provided depending on how the web experience is configured. You can use these example prompts to formulate your own questions and tasks.

Engage with contextual responses

The Amazon Q Business web experience analyzes your questions and returns responses from the selected data sources within your organization. You can continue with a conversation in the context of the active session or start a new conversation to refresh any previous contexts.

Analysis and reasoning

You can ask Amazon Q Business to summarize a response, generate text from a response, do comparative analysis, and perform math and reasoning tasks.

Perform actions using plugins

If your system is configured with **Use a plugin** mode enabled, you can use Amazon Q Business to perform actions on your behalf using plugins. For example, you can ask Amazon Q to schedule a meeting, create a ticket in Jira, or draft an email message. You only see an option to **Use a plugin** in your web experience if your admin has enabled it.

You perform plugin actions by choosing **Use a plugin** mode in your web experience chat. Or, if your admin has enabled the chat orchestration feature, Amazon Q Business automatically orchestrates end user queries across any plugins and data sources you've configured and selects relevant plugin actions. For information about how to use plugins, see Using built-in plugins and Using custom plugins.

> **Note**
>
> You can't use plugins and file uploads at the same time.

Review source citations

The Amazon Q Business web experience provides in-text source citations in a numbered list. To view the source for a response, choose the number at the end of the sentence. The dialog box shows the title, URL, and a snippet from the source that was used to generate the response. Choose the URL to view the source document.

To view the full list of sources, choose **Sources** at the end of the response. You can use the source list to fact-check the response, or for deeper analysis.

Upload files and chat

You can upload document in the Amazon Q Business web experience and ask questions, summarize, or analyze data based on their content. Amazon Q also supports a recent documents list so you can find and reuse recently attached files in new conversations without re-uploading. You can upload new files from your computer, choose from recent files, or drag and drop files directly into a conversation.

A maximum of five files can be uploaded in a single conversation. Documents uploaded through the chat interface are stored in your conversation history and deleted when the conversation is deleted, or after 30 days of inactivity. After files are attached to a conversation, you must delete the conversation to delete the files. You can't delete them individually.

> **Note**
>
> You can't use plugins and file uploads at the same time.

> **Note**
>
> If you connect enterprise data to your application, file upload functionality is only available in the **General Knowledge** section of the web experience and isn't available in the **Company Knowledge** section.

Advanced search

Advanced search is an Amazon Q Business feature that you can toggle on from within your web experience interface. When enabled, it enhances the standard retrieval-augmented generation of Amazon Q Business by employing intelligent agents that analyze queries more thoroughly, maintain conversation context, and intelligently performs multiple data retrieval operations to gather comprehensive information. Advanced search is particularly useful for complex, multi-faceted queries where you need more comprehensive and contextually aware responses, and want to track real time progress on query processing.

For more information, see Agentic Retrieval Augmented Generation (RAG).

Copy responses

You can copy and save the responses for later review and analysis. To copy a response, choose the copy icon at the end of the response.

Provide feedback

You can provide feedback at any time using the feedback button in the left hand sidebar. You can also provide direct feedback about the response you received from the Amazon Q web experience by using the thumbs-up or thumbs-down button. Your feedback is used to help address technical issues in the web experience.

If you select the thumbs-down button, you can choose from the following feedback options:

- **Response is not helpful (incorrect or not relevant to my query)**
- **Response is not based on company documents**
- **Response is not complete**
- **Response is not concise**

- **The sources are inaccurate or missing**
- **Other**

Conversation management

Amazon Q Business stores conversations for up to 30 days, and you can access them in the left navigation pane. You can perform the following tasks to manage your conversations:

- **View conversation history** – Choose a conversation to view the conversation history for that session.
- **Start new conversation** – Choose **+ New conversation** to start a new conversation.
- **Delete conversation** – Choose a conversation that you want to delete, choose **Delete**, and then choose **Delete** again.

Response sources

If you have the appropriate permissions granted by your administrator, you can configure Amazon Q Business web experience responses from up to three sources; **General knowledge**, **Company knowledge**, or from files that you upload.

- **General knowledge** – If you choose this mode, Amazon Q Business only responds using Amazon Q's underlying knowledge.
- **Company knowledge** – If you choose this, Amazon Q Business only responds from your enterprise data.
- **Uploaded files** – If you upload files, Amazon Q Business responds using the data in the files. If the uploaded files don't contain an answer for the query, Amazon Q generates a response from its underlying knowledge.

For more information, see Using global controls in Amazon Q Business.

Login, Logout and session duration for Web Experience

Users log in through their identity provider, which integrates with the Amazon Q Business Web App. After authentication, a session token is generated and the user is automatically logged into the Web App through single sign-on. Amazon Q Business Web App sessions expire one hour after

login. To maintain continuous access, users must refresh their session token before expiration, not after, by refreshing the page.

For security, users should log out of both the Web App and their identity provider when finished. Leaving a session active allows anyone using the same computer within the hour to bypass login due to the still-valid session token.

IDC (Identity Center) Applications

When a user logs out:

- Browser cookies are deleted
- The session is revoked through IDC
- The user is redirected to the login page

IDP (Identity Provider) Applications

When a user logs out:

- Browser cookies are deleted
- The user is redirected to the login page

JWTs (JSON Web Tokens) are used for authentication and authorization and expire after an hour.

> **Note**
>
> If the webpage's cookies are restored after logout, then the IDP session cookie information may still validate the web app, preventing a successful logout.

Amazon Q index for independent software vendors (ISVs)

As an ISV, you can leverage Amazon Q index to access and integrate your customers' enterprise data into your applications. This integration enables you to enhance your applications with generative AI capabilities powered by your customers' data, without having to directly connect to or index individual data sources. Your customers simply need to add you as a data accessor and provide you with the configuration details, allowing you to retrieve relevant content through the `SearchRelevantContent` API operation.

Alternatively, you can create a Amazon Q application environment on behalf of the customer and add their data sources yourself. The Amazon Q index will then be able to retrieve the relevant content through the `SearchRelevantContent` API operation. For more information, see Creating an Amazon Q index on behalf of a customer.

Topics

- Key concepts
- Prerequisites
- Information to be provided to the Amazon Q Business team
- Getting access to your customer's Amazon Q index
- Accessing a customer's Amazon Q index as a data accessor using cross-account access
- Creating an Amazon Q index on behalf of a customer
- Troubleshooting

Key concepts

Amazon Q index

> A comprehensive collection of a company's data that can be queried to build enhanced application experiences. It serves as the foundation for retrieving relevant content across various enterprise data sources.
>
> Organizations that are Amazon Q Business customers and would like to connect their data sources with a supported ISV can add the ISV as a *data accessor*. For more information, see Data accessors.

`SearchRelevantContent` API operation

This API operation enables ISVs to access the Amazon Q index. It supports keyword, semantic, and hybrid queries—allowing for flexible data retrieval options.

AWS Identity and Access Management IAM Identity CenterManaged Application

Amazon Q Business manages end user access to a customer's Amazon Q index using IAWS Identity and Access Management IAM Identity Center.

Resource-based policy

A resource-based policy is an IAM policy that's attached to a resource. Amazon Q Business attaches a resource-based policy to an Amazon Q Business application environment during the data accessor setup. This policy grants the ISV's AWS account the necessary permissions to access content for the customer's end users from the customer's data sources through the `SearchRelevantContent` API operation. By attaching a resource-based policy to the data accessor's AWS account, it allows access to the Amazon Q index of the application environment. For more information, see Data accessors.

Prerequisites

1. Create an AWS account. For more information, see Create an AWS account.
2. Sign up as an independent software provider or vendor (ISV) for Amazon Q index.
3. Complete the AWS verification process to ensure legitimacy and prevent impersonation.
4. The following tabs provide the instructions for how to retrieve your `Tenant ID` for each ISV.

Asana

In Asana, the Tenant ID in Amazon Q Business Data Accessor is called the `domain ID`. You can use the following instructions to retrieve the Asana Tenant ID

1. Choose your account profile picture and select Admin Console.
2. Select Settings.
3. Scroll to Domain Settings to retrieve the Tenant ID.

PagerDuty

In PagerDuty, the tenant ID in Amazon Q Business Data Accessor is called the tenant ID. You can use the following instructions to retrieve the PagerDuty the Tenant ID

1. Select the User Icon.
2. Select Account Settings.
3. Select the PagerDuty Advance tab.
4. Toggle Enable Amazon Q to the on position.
5. The PagerDuty Tenant ID is now available from the Amazon Q Business Configuration Values modal.

Kore.ai (AIforWork)

In AIforWork, the Tenant ID is displayed directly in the setup form. You can use the following instructions to retrieve the Kore.ai Tenant ID:

1. Navigate to AIforWork platform.
2. When setting up an Enterprise Knowledge or Search Agent, choose **Q for Business**.
3. In the setup form that opens, the Tenant ID is displayed and ready to copy.

Revinova

The Portal ID in Revinova is the Tenant ID for Amazon Q Business Data Accessor. You can use the instructions below to retrieve the Portal ID from Revinova.

1. Log in to the admin console.
2. Navigate to the portals dashboard using the **Portals** menu under the settings menu collection.
3. In the portal's grid, hover on the header of any of the columns and click on the hamburger menu shown in the column to open the column options context menu.
4. Click on the grid icon available on the top right corner of the column options context menu.
5. Select **ID** from the list of columns available for display, and it will show the portal IDs in the grid.
6. You can get the ID for the portal from the corresponding row.

Planview

Your Planview Tenant ID is a unique identifier in UUID/GUID format (e.g., 12345678-1234-1234-1234-123456789abc).

For Planview, the Tenant ID information can be found in their integration documentation. You can use the following resource to retrieve the Tenant ID for Planview Viz integration with Amazon Q Business.

1. Refer to the Planview Amazon Q Business Integration FAQ for detailed instructions on retrieving your Tenant ID.

> **Note**
>
> Planview data accessor is only available in the `us-west-2` region.

Amplience

For Amplience, the Tenant ID is the Hub ID. You can use the following instructions to retrieve the Amplience Tenant ID.

1. Within Amplience Dynamic Content, switch into the Hub you wish to connect.
2. Select the settings icon in the top right corner and select the **Properties** menu item.
3. The Hub ID will be displayed with a copy to clipboard option.

Saviynt

For Saviynt, the Tenant ID is the FQDN from the Saviynt Console. You can use the following instructions to retrieve the Saviynt FQDN.

The URL will look similar to this example https://ispm-dev.saviyntcloud.com/ and the tenant id from this example will be "ispm-dev.saviyntcloud.com"

Webex by CISCO

In Webex, the tenant ID in Amazon Q Business Data Accessor is called the Organization ID. You can use the following instructions to retrieve the Webex Tenant ID.

1. Login in Cisco Control Hub.

2. Go to Account->Info page.
3. Copy the Organization ID.

Fireflies.ai

When prompted for Tenant ID, please enter Team ID

Miro

For Miro, the Tenant ID is Organization ID. Organization admins can navigate to the 'Organization profile' page and get the id from the address bar.

SUSE Rancher for Amazon Web Services

For SUSE Rancher for Amazon Web Services, the Tenant ID is tenant-uid. The tenant-uid can be found within the application in the about info in the top right of the screen.

CXone Mpower

For CXone Mpower, the Tenant ID required for the Amazon Q Business Data Accessor is displayed on your My Profile page. To access this page,

- In the upper-right corner of any page in the platform, click your initials.

- Select My Profile from the menu.

- On the General tab of the My Profile page, locate your Tenant ID.

Information to be provided to the Amazon Q Business team

Before an independent software provider or vendor (ISV) can become a verified data accessor, they must provide either an Auth code or Trusted token issuer (TTI) configuration information to the Amazon Q Business team.

Prerequisite for both Auth code and TTI configurations.

`tenantID`

The `tenantID` is a unique identifier for your application tenant. Each application might have different terms for a tenant such as Workspace ID for Slack or Domain ID for Asana. You can review the Prerequisites page to see how to retrieve the `TenantId` for your application.

Auth code

Prerequisites:

- The display name to list on the AWS Management Console
- The business logo that Amazon Q Business customers will select
- The redirect URL for the oAuth authorization code flow.

> **Note**
>
> oAuth authorization code flow is an industry standard for third-party applications to obtain user access permissions. In the authorization code flow, ISV receives an auth code from AWS and exchanges the auth code for an ID token.

- The ISVs must create the following AWS Identity and Access Management (IAM) role with the necessary permissions and trust policy to interact with the Amazon Q Business services and APIs. This IAM role is granted access as a data accessor when Amazon Q Business customers provide access to their Amazon Q index. For more information, see IAM role terms and concepts and Create a role to delegate permissions to an IAM user.
  - **ISV IAM role**

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "qbusiness:SearchRelevantContent",
                "sso-oauth:CreateTokenWithIAM",
                "kms:Decrypt",
                "sts:SetContext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "MultiServicePermissions"
        }
    ]
}
```

  - **ISV IAM role trust policy**

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ISVRoleTrustPolicy",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/YourApplicationRole"
                ]
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext",
                "sts:TagSession"
            ]
        }
    ]
}
```

- ISV `tenantId`
  - What is `tenantId`?

    The `tenantID` is a unique identifier for your application tenant. Each application might have different terms for a tenant such as Workspace ID for Slack or Domain ID for Asana.
  - Where do you find the `tenantId`?

    Provide info as to where can the IT Admin of an enterprise can find this information on the ISV.

TTI

Prerequisites:

- The display name to list on the AWS Management Console
- The business logo that Amazon Q Business customers will select
- OIDC ClientId which can used to generate tokens for all the customers - The OAuth 2.0 authorization server (the trusted token issuer) that creates the token must have an OpenID Connect (OIDC) discovery endpoint that IAM Identity Center can use to obtain public keys to

verify the token signatures. For more information, see OIDC discovery endpoint URL (issuer URL).

- Discovery endpoint/Issuer URL - The entity that issued the token. This value must match the value that is configured in the OIDC discovery endpoint (issuer URL) in the trusted token issuer.

> **Note**
>
> Trusted token issuer(App level authentication) - A trusted token issuer is an OAuth 2.0 authorization server that creates signed tokens. These tokens authorize applications that initiate requests (requesting applications) for access to AWS managed applications (receiving applications).

The ISVs must create the following AWS Identity and Access Management (IAM) role with the necessary permissions and trust policy to interact with the Amazon Q Business services and APIs. This IAM role is granted access as a data accessor when Amazon Q Business customers provide access to their Amazon Q index. For more information, see IAM role terms and concepts and Create a role to delegate permissions to an IAM user.

- **ISV IAM role**

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "qbusiness:SearchRelevantContent",
                "sso-oauth:CreateTokenWithIAM",
                "kms:Decrypt",
                "sts:SetContext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "MultiServicePermissions"
        }
    ]
```

```
}
```

- **ISV IAM role trust policy**

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ISVRoleTrustPolicy",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/YourApplicationRole"
                ]
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext",
                "sts:TagSession"
            ]
        }
    ]
}
```

Getting access to your customer's Amazon Q index

There are two non-mutually exclusive ways to get access to a customer's Amazon Q index:

Customer grants ISVs (data accessors) access to their Amazon Q index

Amazon Q Business customers add the ISV as a *data accessor* to their Amazon Q Business application environment and underlying Amazon Q index. This includes Amazon Q customers selecting which data sources and end users can retrieve data from and grant ISVs *cross-account* access to their Amazon Q index based on those permissions.

> **Note**
>
> Only ISVs who successfully complete registration with Amazon Q Business can be listed as data accessors.

Only Amazon Q Business application environments that are created using AWS Identity and Access Management (IAM) identity center (IDC) are supported.

This process gives Amazon Q customers more flexibility, oversight, and control of their Amazon Q index. Amazon Q customers can create their Q index once, and then grant multiple ISVs access to the same minimizing replication of enterprise data and permissions across multiple ISVs. For more information, see Data accessors and Accessing a customer's Amazon Q index as a data accessor using cross-account access.

The ISV sets up the Amazon Q index on behalf of the customer within their own AWS account

ISVs can manage the entire process themselves, creating an Amazon Q Business application environment and the underlying Amazon Q index on behalf of each customer in their AWS account. Customers must provide ISV credentials to connect to their data sources.

At the end of both workflows, ISVs can retrieve the data that they have access to using the Amazon Q index.

Comparison of onboarding options

Scenario	Onboarding with Amazon Q Business	Onboarding with the ISV
Where is the Amazon Q Business application environment created?	Amazon Q Business customer's account	ISV's account
Who sets up Amazon Q Business application environment and underlying Amazon Q index?	Amazon Q Business customer	ISV on behalf of the customer

We recommend that ISVs use both onboarding workflows to best support all customers.

Accessing a customer's Amazon Q index as a data accessor using cross-account access

After Amazon Q Business customers give an independent software provider or vendor's (ISV) *data accessor* permissions to retrieve data from their Amazon Q index, the customer or the ISV must connect with one another to get the following configuration details. These configuration parameters are required inputs when they use the `SearchRelevantContent` API operation to perform cross-account access to relevant data from the customer's Amazon Q index. These parameters are accessed from the customer's Amazon Q console in the **Information for data accessor** tab in the **data accessor details** page which is accessed by choosing the accessor **Name** from the **Data accessors** table on the **Data accessors** page of their application environment.

1. Amazon Q Business application ID — This is unique identifier of the Amazon Q Business application environment. It tells the ISV what Amazon Q application environment is associated with the Amazon Q index.
2. The Amazon Q Business application Region — This is the AWS Region where the Amazon Q Business application environment is created.
3. Amazon Q Business retriever ID — This is unique identifier for the retriever. The retriever gets the data from the Amazon Q index configured by the Amazon Q customer.
4. Data accessor application ARN — This is the ISV Amazon Resource Name (ARN). It is used to identify the ISV when it is accessing a customer's Amazon Q index.
5. The Region for the Identity and Access Management (IAM) Identity Center (IDC) instance — This is the AWS Region where the IDC instance of the customer has been created.

With these parameters, the ISV can begin retrieving content from the Amazon Q index by calling the `SearchRelevantContent` API operation. The `SearchRelevantContent` API operation follows Amazon Q Business access control standards by only retrieving data that the customer's end users have been given access to.

Retrieving data from a customer's Amazon Q index as a data accessor using the SearchRelevantContent API

With valid configuration parameters from the customer, the ISV can use the `SearchRelevantContent` API operation to retrieve user-specific content from the customer's Amazon Q index.

The following are examples of how to use either Auth Code or Trusted Token Issuer based authentication (TTI) to complete this task:

The following tabs provide a procedure to boost document attributes using the console and code examples for the AWS CLI.

Auth code

Use the Authentication code method to retrieve user-specific content from the customer's Amazon Q index.

1. The Amazon Q index customer's end user will login to the ISV's application using the existing user login flow.

   > **Note**
   >
   > The ISV doesn't need to change their existing login flow.

2. After the end user successfully logs in, the ISV instructs the user to authenticate to their Amazon Q index through their OIDC providers. For more information, see Creating an Amazon Q Business application using AWS IAM Identity Center.

   a. `https://oidc.${idc_region}.amazonaws.com/authorize?response_type=code&redirect_uri=${isv_redirect_url}&state={oauth_state}&client_id=${idc_application_arn}`

   b. `isv_redirect_uri` — This is the *redirect URL* that's registered at the ISV registration process. For more information, see Information to be provided to the Amazon Q Business team.

   c. `oauth_state` — This random string prevents cross-site request forgery (CSRF) attack. For more detail about state parameters in oauth, see Prevent Attacks and Redirect Users with OAuth 2.0 State Parameters in the auth by Okta guide.

   d. `idc_application_arn` — This is the Amazon Q Business DataAccessor IAM Identity Center application ID that's provided by the customer to the ISV.

3. The end user logs in using the method configured by the customer's Amazon Q administrator. For example, the user's company SSO.

4. The ISV application receives an *auth code* in their *redirect URL*.

5. The ISV application calls the `CreateTokenWithIAM` API operation to get a token with an authorization code. The ISV needs to use the AWS Identity and Access Management (IAM) role that they created during the onboarding process with `tenantId` information in the tags like the following:

```
aws sts assume-role \
      --role-arn ${your_iam_role} \
      --role-session-name test-session \
      --tags Key=qbusiness-dataaccessor:ExternalId,Value=${isv tenantId}

aws sso-oidc create-token-with-iam --client-id "${idc_application_arn}" \
      --redirect-uri "{your_redirect_uri}" \
      --grant-type "authorization_code" \
      --code "${CODE}" --region ${idc_region}
```

6. Get the `idToken` field from the response of `CreateTokenWithIAM`. Then, decode the `idToken` and extract `"sts:identity_context"` field from it.

   Using command line:

```
export ID_TOKEN_I = "${response_json_of_create-token-with-iam}"
export ID_CONTEXT=`jq -R 'split(".") | .[1] | @base64d | fromjson' <<<
 "$ID_TOKEN_I" | jq -r '."sts:identity_context"'`
echo "ID_CONTEXT=$ID_CONTEXT\n"
```

   Using Python:

```
import json
import base64

body = "${response_json_of_create-token-with-iam}"
body_json = base64.urlsafe_b64decode(body.split(".")[1] + '==')
data = json.loads(body_json)
print(f"{data['sts:identity_context']}")
```

7. Call the AssumeRole API with the extracted `sts:identity_context` and the ISV `tenantId` information.

```
aws sts assume-role \
      --role-arn ${your_iam_role} \
      --role-session-name test-session \
      --provided-contexts '[{"ProviderArn": "arn:aws:iam::aws:contextProvider/
IdentityCenter", "ContextAssertion": "${value from sts:identity_context}"}]' \
      --tags Key=qbusiness-dataaccessor:ExternalId,Value=${isv tenantId}
```

8. Use the AWS Sig V4 credentials returned from the previous step to call `SearchRelevantContent` API.

```
aws qbusiness search-relevant-content \
      --application-id ${qbusiness_application_id} \
      --query-text "What is Amazon Q?" \
      --content-source '{"retriever": {"retrieverId": "${retriever_id}"}}'
```

TTI

Use the Trusted Token Issuer based authentication (TTI) method to retrieve user-specific content from the customer's Amazon Q index.

1. The Amazon Q index customer's end user will log in to the ISV's application using the existing user login flow.
2. After the end user successfully logs in, ISV issues a token for the end user using the OIDC client as audience, provided during the onboarding process.
3. The ISV application calls the `CreateTokenWithIAM` API operation with the token from step 2. The ISV needs to use the AWS Identity and Access Management (IAM) role that they created during the onboarding process with `tenantId` information in the tags like the following:

```
aws sts assume-role \
      --role-arn ${your_iam_role} \
      --role-session-name test-session \
      --tags Key=qbusiness-dataaccessor:ExternalId,Value=${isv tenantId}
```

```
aws sso-oidc create-token-with-iam --client-id "${idc_application_arn}" \
      --grant-type "urn:ietf:params:oauth:grant-type:jwt-bearer" \
      --assertion "${isv token generated using oidc client provided during
 onboarding}" --region ${idc_region}
```

4. Retrieve the `idToken`field from the response of `CreateTokenWithIAM`. Then, decode the `idToken` and extract `sts:identity_context` field from it.

   a. Using command line:

   ```
   export ID_TOKEN_I = "${response_json_of_create-token-with-iam}"
   export ID_CONTEXT=`jq -R 'split(".") | .[1] | @base64d | fromjson' <<<
    "$ID_TOKEN_I" | jq -r '."sts:identity_context"'`
   echo "ID_CONTEXT=$ID_CONTEXT\n"
   ```

   b. Using Python:

   ```
                                              import json
   import base64

   body = "${response_json_of_create-token-with-iam}"
   body_json = base64.urlsafe_b64decode(body.split(".")[1] + '==')
   data = json.loads(body_json)
   print(f"{data['sts:identity_context']}")
   ```

5. Call the `AssumeRole` API with the extracted `sts:identity_context` and the ISV `tenantId` information.

   ```
   aws sts assume-role \
         --role-arn ${your_iam_role} \
         --role-session-name test-session \
         --provided-contexts '[{"ProviderArn": "arn:aws:iam::aws:contextProvider/
   IdentityCenter", "ContextAssertion": "${value from sts:identity_context}"}]' \
         --tags Key=qbusiness-dataaccessor:ExternalId,Value=${isv tenantId}
   ```

Use the AWS Sig V4 credentials returned from the previous step to call `SearchRelevantContent` API.

```
aws qbusiness search-relevant-content \
      --application-id ${qbusiness_application_id} \
      --query-text "What is Amazon Q?" \
      --content-source '{"retriever": {"retrieverId": "${retriever_id}"}}'
```

Creating an Amazon Q index on behalf of a customer

We recommend creating one Amazon Q Business application environment per customer for better security and data segregation. Alternatively, you can create one Amazon Q Business application environment and share it with multiple customers. This is only recommended when you index documents that are visible to all users in your application.

Topics

- Determine the identity management for your customer's Amazon Q Business application
- Calling the SearchRelevantContent API to an Amazon Q index with an IAM Identity Center application environment
- Calling the SearchRelevantContent API on an Amazon Q application environment with IAM Federation

Determine the identity management for your customer's Amazon Q Business application

All Amazon Q Business application environments require user access through AWS Identity and Access Management (IAM) identity management. You can choose one of two types of user IAM identity management methods supported by Amazon Q Business. These are IAM Identity Center and IAM Federation. Both IAM Identity Center and IAM Federation require an external identity provider setup to allow end users to log in through their identity provider.

IAM Identity Center provides advanced user group management, while Identity and Access Management (IAM) Federation provides more service quotas for the external identity providers. You can choose the identity management that's best suited for you and your end customer when creating their Amazon Q Business application environment. For more information, see Configuring an Amazon Q Business application environment using AWS IAM Identity Center and Creating an Amazon Q Business application environment using Identity Federation through IAM

After the Amazon Q Business application environment is created, set up the retriever and connect the data sources. For a complete list of data source connectors,see supported connectors. You will need your customers to provide the relevant credentials for each connector that you intend to retrieve data from. For more information, see Creating a retriever for an Amazon Q Business application and Connecting Amazon Q Business data sources.

Calling the SearchRelevantContent API to an Amazon Q index with an IAM Identity Center application environment

Before end users can retrieve content from the Amazon Q index that you have been granted access to, you need to be able to make authenticated Amazon Q Business API calls, like the `SearchRelevantContent` API operation.

To do this you, must complete the steps in Make authenticated Amazon Q Business API calls using IAM Identity Center.

> **Note**
>
> Use the instructions from the previous topic, but modify the `QBusinessConversationPermission` permission by adding the additional action , `"qbusiness:SearchRelevantContent"` to the list of allowed actions, as shown in the following sample snippet of the full permission.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessConversationPermission",
```

```
            "Effect": "Allow",
            "Action": [
                "qbusiness:Chat",
                "... ",
                "qbusiness:SearchRelevantContent"
            ]
        }
    ]
}
```

When configuring access scopes for your Amazon Q Businessapplication environment, add the following using the AWS CLI to enable calling the `SearchRelevantContent` API:

```
aws sso-admin put-application-access-scope \
--application-arn identity-center-custom-application-arn \
--scope "qbusiness:conversations:access"

aws sso-admin put-application-access-scope \
--application-arn identity-center-custom-application-arn \
--scope "qbusiness:content:access"
```

The following AWS CLI example shows how to call this `SearchRelevantContent` API operation after you have these credentials.

```
aws qbusiness search-relevant-content \
  --application-id ${qbusiness_application_id} \
  --query-text "What is Amazon Q?" \
  --content-source '{"retriever": {"retrieverId": "${retriever_id"}}'
```

Calling the SearchRelevantContent API on an Amazon Q application environment with IAM Federation

Before end users can retrieve content from the Amazon Q index that you have been granted access to, you need to be able to make authenticated Amazon Q Business API calls, like the `SearchRelevantContent` API operation.

To do this, complete the steps in Make authenticated Amazon Q Business API calls using IAM federation.

Note

Use the instructions in the previous topic, but modify the `trustpolicyforfederation` policy by adding the additional action, `"qbusiness:SearchRelevantContent"` to the list of allowed actions, as shown in the following sample snippet of the full permission.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessConversationPermissions",
            "Effect": "Allow",
            "Action": [
                "qbusiness:Chat",
                "qbusiness:SearchRelevantContent"
            ],
            "Resource": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
        }
    ]
}
```

The following AWS CLI; example shows how to call this `SearchRelevantContent` API operation after you have these credentials.

```
aws qbusiness search-relevant-content \
  --application-id ${qbusiness_application_id} \
  --query-text "What is Amazon Q?" \
  --content-source '{"retriever": {"retrieverId": "${retriever_id"}}'
```

Troubleshooting

If ISVs encounter issues with accessing the Amazon Q index, consider the following.

1. Verify the Identity and Access Management (IAM) role and permissions.
2. Check the configuration of the redirect URL for the oauth flow.
3. Confirm that the customer has granted the necessary access permissions to the ISV.

Security in Amazon Q Business

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from data centers and network architectures that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to Amazon Q Business, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon Q Business. The following topics show you how to configure Amazon Q Business to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Amazon Q Business resources.

Topics

- Data protection in Amazon Q Business
- Amazon Q Business and interface Amazon VPC endpoints (AWS PrivateLink)
- Identity and access management for Amazon Q Business
- Compliance validation for Amazon Q Business
- Using ACL Analyzer in Amazon Q
- Resilience in Amazon Q Business
- Infrastructure security in Amazon Q Business
- Cross-service confused deputy prevention
- Configuration and vulnerability analysis in AWS Identity and Access Management
- Security best practices

Data protection in Amazon Q Business

The AWS shared responsibility model applies to data protection in Amazon Q Business. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail. For information about using CloudTrail trails to capture AWS activities, see Working with CloudTrail trails in the *AWS CloudTrail User Guide*.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-3 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-3.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with Amazon Q or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Data encryption for Amazon Q Business

Amazon Q Business supports encryption at rest using a customer supplied symmetric AWS KMS key when provided, or uses an AWS-owned AWS KMS key if no customer managed key is provided. Amazon Q Business also uses HTTPS protocol for data in transit.

> **Important**
>
> Amazon Q does not support asymmetric KMS keys. For more information, see Using Symmetric and Asymmetric Keys in the *AWS Key Management Service Developer Guide*.

Topics

- Encryption at rest
- Encryption in transit

Encryption at rest

Amazon Q Business provides encryption by default to protect sensitive customer data at rest using AWS owned encryption keys. Sensitive customer data includes both questions and answers in the Amazon Q Business web experience and the documents uploaded to Amazon Q Business index.

The Amazon Q Business uses the questions and answers to know the conversation context and to provide you with the best answer. The conversation data is automatically removed once the conversation is deleted or is inactive. For more information, see Conversation management. The uploaded documents are used by Amazon Q Business to retrieve them at runtime to answer your questions.

- **AWS owned keys** – Amazon Q Business uses these keys by default to automatically encrypt sensitive customer data. You can't view, manage, or use AWS owned keys, or audit their use. However, you don't have to take any action or change any programs to protect the keys that encrypt your data. For more information, see AWS owned keys in the *AWS Key Management Service Developer Guide*.

  Encryption of data at rest by default helps reduce the operational overhead and complexity involved in protecting sensitive data. At the same time, it enables you to build secure applications that meet strict encryption compliance and regulatory requirements.

While you can't disable this layer of encryption or select an alternate encryption type, you can add a second layer of encryption over the existing AWS owned encryption keys by choosing a customer managed key when you create your resources:

- **AWS KMS key (KMS)** – Amazon Q supports the use of symmetric customer managed keys that you create, own, and manage to add a second layer of encryption over the existing AWS owned encryption.

  In Amazon Q Business, you configure KMS keys when you create an Amazon Q Business application environment. The same KMS key is used to encrypt data for the application environment you create and any child resources under the application environment (for example, an Amazon Q Business index). However, KMS keys are not supported for the Amazon Q Business Starter index. So, if you use a KMS key with your application environment, you won't be able to use an Amazon Q Business Starter index for it. To use KMS keys, you must choose either an Amazon Q Business Enterprise index or an Amazon Kendra retriever for your application environment.

> **Important**
>
> Amazon Q does not support asymmetric KMS keys. For more information, see Using Symmetric and Asymmetric Keys in the *AWS Key Management Service Developer Guide*.

Because you have full control of this layer of encryption, you can perform such tasks as:

- Establishing and maintaining key policies
- Establishing and maintaining IAM policies and grants
- Enabling and disabling key policies
- Rotating key cryptographic material
- Adding tags
- Creating key aliases
- Scheduling keys for deletion

For more information, see customer managed key in the *AWS Key Management Service Developer Guide*.

> **Note**
>
> If you have created your Amazon Q Business application environment using AWS KMS and then you want to migrate to using customer managed key (CMK), you will have to re-create your application environment.

Topics

- How Amazon Q Business uses grants in AWS KMS
- Create a customer managed key
- Specifying customer managed key for Amazon Q Business
- Monitoring your encryption keys for Amazon Q

How Amazon Q Business uses grants in AWS KMS

Amazon Q Business requires a grant to use your customer managed key. When you create a Amazon Q Business application environment resource encrypted with a customer managed key, Amazon Q creates a grant on your behalf by sending a CreateGrant request to AWS KMS. Grants in AWS KMS are used to give Amazon Q Business access to a KMS key in a customer account.

Amazon Q Business requires the grant to use your customer managed key for the following internal operations:

- Send DescribeKey requests to AWS KMS to verify that the symmetric customer managed key ID entered when creating application environment is valid.
- Send GenerateDataKeyWithoutPlainText requests to AWS KMS to generate data keys encrypted by your customer managed key.
- Send Decrypt requests to AWS KMS to decrypt the encrypted data keys so that they can be used to encrypt your data.

You can revoke access to the grant, or remove the service's access to the customer managed key at any time. If you do, Amazon Q Business won't be able to access any of the data encrypted by the customer managed key, which affects operations that are dependent on that data.

Create a customer managed key

You can create a symmetric customer managed key by using the AWS Management Console, or the AWS KMS APIs.

> **Important**
>
> Amazon Q does not support asymmetric KMS keys. For more information, see Using Symmetric and Asymmetric Keys in the *AWS Key Management Service Developer Guide*.

To create a symmetric customer managed key

Follow the steps for Creating symmetric customer managed key in the *AWS Key Management Service Developer Guide*.

Key policy

Key policies control access to your customer managed key. Every customer managed key must have exactly one key policy, which contains statements that determine who can use the key and how they can use it. When you create your customer managed key, you can specify a key policy. For more information, see Managing access to customer managed keys in the *AWS Key Management Service Developer Guide*.

To use your customer managed key with your Amazon Q Business resources, the following API operations must be permitted in the key policy:

- kms:CreateGrant – Adds a grant to a customer managed key. Grants control access to a specified KMS key,which allows access to grant operation Amazon Q Business requires. For more information about Using Grants, see the *AWS Key Management Service Developer Guide*.

  This allows Amazon Q Business to do the following:

  - Call `GenerateDataKeyWithoutPlainText` to generate an encrypted data key and store it, because the data key isn't immediately used to encrypt.
  - Call `Decrypt` to use the stored encrypted data key to access encrypted data.
  - Set up a retiring principal to allow the service to `RetireGrant`.
- kms:DescribeKey – Provides the customer managed key details to allow Amazon Q to validate the key.

The following are policy statement examples you can add for Amazon Q Business

```
"Statement": [{
        "Sid": "Allow access to principals authorized to use Amazon Q",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::111122223333:role/Admin"
        },
        "Action": [
            "kms:DescribeKey",
            "kms:CreateGrant"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "kms:ViaService": "qbusiness.region.amazonaws.com",
                "kms:CallerAccount": "111122223333"
            }
          }
        },
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:*"
            ],
            "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
        },
        {
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*",
                "kms:RevokeGrant"
            ],
            "Resource": "*"
```

```
        }
    ]
```

For more information about specifying permissions in a policy and troubleshooting key access, see the *AWS Key Management Service Developer Guide*

Specifying customer managed key for Amazon Q Business

You can specify a customer managed key as a second layer encryption for your Amazon Q Business application environment resource.

When you create your application environment, you can specify the data key by entering a **KMS ID**, which Amazon Q Business uses to encrypt the identifiable personal data stored by the application environment.

KMS ID – A key identifier for an AWS KMS customer managed key. Enter a key ID, key ARN, alias name, or alias ARN.

Any resources you create under your Amazon Q Business application environment will be encrypted with the same key.

Monitoring your encryption keys for Amazon Q

When you use an AWS KMS customer managed key with your Amazon Q Business resources, you can use AWS CloudTrail or Amazon CloudWatch Logs to track requests that Amazon Q Business sends to AWS KMS.

The following examples are AWS CloudTrail events for `CreateGrant`, `GenerateDataKey`, `Decrypt`, and `DescribeKey` to monitor KMS operations called by Amazon Q Business to access data encrypted by your customer managed key.

CreateGrant

When you use an AWS KMS customer managed key to encrypt your application environment, Amazon Q sends a `CreateGrant` request on your behalf to access the KMS key in your AWS account. The grant that Amazon Q Business creates are specific to the resource associated with the AWS KMS customer managed key. In addition , Amazon Q Business uses the `RetireGrant` operation to remove a grant when you delete a resource.

The following example event records the `CreateGrant` operation:

```
{
```

```
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
            "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/
Sampleuser01",
                    "accountId": "111122223333",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2021-04-22T17:02:00Z"
                }
            },
            "invokedBy": "qbusiness.amazonaws.com"
        },
        "eventTime": "2021-04-22T17:07:02Z",
        "eventSource": "kms.amazonaws.com",
        "eventName": "CreateGrant",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "172.12.34.56",
        "userAgent": "ExampleDesktop/1.0 (V1; OS)",
        "requestParameters": {
            "retiringPrincipal": "qbusiness.region.amazonaws.com",
            "operations": [
                "CreateGrant",
                "RetireGrant",
                "GenerateDataKey",
                "GenerateDataKeyWithoutPlaintext",
                "Encrypt",
                "ReEncryptTo",
                "ReEncryptFrom",
                "Decrypt",
                "DescribeKey"
            ],
```

```
            "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
            "granteePrincipal": "qbusiness.region.amazonaws.com"
        },
        "responseElements": {
            "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE"
        },
        "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
        "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
        "readOnly": false,
        "resources": [
            {
                "accountId": "111122223333",
                "type": "AWS::KMS::Key",
                "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
            }
        ],
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "eventCategory": "Management",
        "recipientAccountId": "111122223333"
    }
```

GenerateDataKey

When you use an AWS KMS customer managed key for your application environment, Amazon Q Business creates a unique table key. It sends a `GenerateDataKey` request to AWS KMS that specifies the AWS KMS customer managed key for the application environment.

The following example event records the `GenerateDataKey` operation:

```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AWSService",
            "invokedBy": "qbusiness.amazonaws.com"
        },
        "eventTime": "2023-11-24T01:50:25Z",
        "eventSource": "kms.amazonaws.com",
        "eventName": "GenerateDataKey",
        "awsRegion": "us-west-2",
```

```
        "sourceIPAddress": "172.12.34.56",
        "userAgent": "ExampleDesktop/1.0 (V1; OS)",
        "requestParameters": {
            "keyId": "arn:aws:kms:us-west-2:398547360552:key/ba6c9092-
ad4d-41c3-937a-f02177ae147e",
            "keySpec": "AES_256"
        },
        "responseElements": null,
        "requestID": "4bd8e018-90d0-4b93-bc8d-32338578a158",
        "eventID": "aca6cb5b-44bb-3ed6-afdd-736432323356",
        "readOnly": true,
        "resources": [
            {
                "accountId": "111122223333",
                "type": "AWS::KMS::Key",
                "ARN": "arn:aws:kms:us-west-2:398547360552:key/ba6c9092-
ad4d-41c3-937a-f02177ae147e"
            }
        ],
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "398547360552",
        "sharedEventID": "57393866-c398-4fd6-a259-d6cb001c7cf9",
        "eventCategory": "Management"
    }
```

Decrypt

When you access an encrypted application environment, Amazon Q Business calls the `Decrypt` operation to use the stored encrypted data key to access the encrypted data.

The following example event records the `Decrypt` operation.

```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AWSService",
            "invokedBy": "qbusiness.amazonaws.com"
        },
        "eventTime": "2021-04-22T17:10:51Z",
        "eventSource": "kms.amazonaws.com",
        "eventName": "Decrypt",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "172.12.34.56",
```

```
        "userAgent": "ExampleDesktop/1.0 (V1; OS)",
        "requestParameters": {
            "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
            "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
        },
        "responseElements": null,
        "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
        "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
        "readOnly": true,
        "resources": [
            {
                "accountId": "111122223333",
                "type": "AWS::KMS::Key",
                "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
            }
        ],
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "eventCategory": "Management",
        "recipientAccountId": "111122223333",
        "sharedEventID": "dc129381-1d94-49bd-b522-f56a3482d088"
    }
```

DescribeKey

Amazon Q Business uses the `DescribeKey` operation to verify if the AWS KMS customer managed key associated with your application environment exists in the account and region.

The following example event records `DescribeKey` operation:

```
    {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
            "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
```

```
                    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/
Sampleuser01",
                    "accountId": "111122223333",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2021-04-22T17:02:00Z"
                }
            },
            "invokedBy": "qbusiness.amazonaws.com"
        },
        "eventTime": "2021-04-22T17:07:02Z",
        "eventSource": "kms.amazonaws.com",
        "eventName": "DescribeKey",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "172.12.34.56",
        "userAgent": "ExampleDesktop/1.0 (V1; OS)",
        "requestParameters": {
            "keyId": "00dd0db0-0000-0000-ac00-b0c000SAMPLE"
        },
        "responseElements": null,
        "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
        "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
        "readOnly": true,
        "resources": [
            {
                "accountId": "111122223333",
                "type": "AWS::KMS::Key",
                "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
            }
        ],
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "eventCategory": "Management",
        "recipientAccountId": "111122223333"
    }
```

Encryption in transit

Amazon Q Business uses the HTTPS protocol to communicate with your client application environment. It uses HTTPS and AWS Signature Version 4 (SigV4) to communicate with other services on your application environment's behalf.

Topics

- Data encryption for Q Apps
- Key management
- Cross-region inference in Amazon Q Business
- Amazon Q Business Service improvement

Data encryption for Q Apps

Q Apps stores the following data:

- Title and description of the Q Apps.
- Titles of the individual cards.
- Prompts the builders may specify for the “Text output” cards.
- Any files uploaded as default values for “File upload” cards.
- The data that users put into the “Text input” cards when running the Q Apps.
- Any files uploaded by users when running the Q Apps.

When you create a Amazon Q Business "application" as the application environment for Q Apps after April 30th 2024, Q Apps will be enabled out of the box. If a customer managed key is not configured, then Q Apps encrypts all the above data using AWS-owned keys. For more information, see AWS owned keys in the *AWS Key Management Service Developer Guide*.

> **Note**
>
> If you configure a customer managed key when creating an Amazon Q Business application environment, then Q Apps uses the same customer managed key to encrypt all of the above data in Q Apps as well.

Q Apps requires a grant to use your customer managed key. When you create an Amazon Q Business application environment resource encrypted with a customer managed key, Q Apps, creates a grant on your behalf by sending a `CreateGrant` request to AWS KMS. Grants in AWS KMS are used to give Q Apps, access to a KMS key in a customer account.

Q Apps requires the grant to use your customer managed key for the following internal operations:

- Send `DescribeKey` requests to AWS KMS to verify that the symmetric customer managed key ID entered when creating application environment is valid.
- Send `GenerateDataKeyWithoutPlainText` requests to AWS KMS to generate data keys encrypted by your customer managed key.
- Send `Decrypt` requests to AWS KMS to decrypt the encrypted data keys so that they can be used to encrypt your data.

You can revoke access to the grant, or remove the service's access to the customer managed key at any time. If you do, Q Apps won't be able to access any of the data encrypted by the customer managed key, which affects operations that are dependent on that data.

> **Note**
>
> Q Apps has a different service principal and Q Apps creates a different grant from the grant created for "Amazon Q Business". You can specifically revoke access to the grant for "Q Apps" without revoking access to the grant for "Amazon Q Business" or vice versa.

Enabling Q Apps on Q applications created before April 30th 2024

If you have already configured a Amazon Q Business application environment to use a customer managed key, when you enable Q Apps feature in the web experience for the first time, under the global controls, a new grant shall be created to the same customer managed key specified when configuring data encryption Amazon Q Business.

Note that disabling Q Apps in the web experience will not automatically revoke this grant because administrators can still list and delete Q Apps in the admin console, even though Q Apps web experience is disabled. But if you delete the Amazon Q Business application environment altogether, then both grants to `qbusiness` and `qapps` shall be revoked.

You can always revoke access to both the grants or remove access to the customer managed key at any time.

Key management

Amazon Q Business encrypts the contents of your index using the following types of keys:

- An AWS-owned AWS KMS. This is the default.
- A customer-managed KMS key. You can create the key when you are creating an Amazon Q application environment, retriever, index, web experience, data source, or plugins, or you can create the key using the AWS KMS console. Select a symmetric encryption customer-managed KMS key.

> **Important**
>
> Amazon Q does not support asymmetric KMS keys. For more information, see Using Symmetric and Asymmetric Keys in the *AWS Key Management Service Developer Guide*.

Cross-region inference in Amazon Q Business

With cross-region inference, Amazon Q Business will automatically select the optimal region within your geography (as described in more detail below) to process your inference request, maximizing available compute resources and model availability, and providing the best customer experience. With cross-region inference, you get:

- Complete access to most advanced Amazon Q Business AI capabilities and features
- Access to a variety of models suitable for different tasks
- Improved performance for all your applications

Cross-region inference requests are kept within the AWS Regions that are part of the geography where the data originally resides. For example, a request made within the US is kept within the AWS Regions in the US. Although the data remains stored only in the primary region, when using cross-region inference, your input prompts and output results may move outside of your primary region. All data will be transmitted encrypted across Amazon's secure network.

Important

Cross-region inference is enabled by default for Amazon Q Business applications. For customers with highly regulated workloads that need to keep data processing resident in-country, contact AWS Support.

Note

There's no additional cost for using cross-region inference.
Amazon CloudWatch and AWS CloudTrail logs won't specify the AWS Region in which data inference occurs.

Supported regions for Amazon Q Business cross-region inference

For a list of Region codes and endpoints supported in Amazon Q Business, see Amazon Q Business endpoints and quotas.

Supported Amazon Q Business geography	Inference regions
United States	US East (N. Virginia) (us-east-1) US West (Oregon) (us-west-2)
Europe	Europe (Frankfurt) (eu-central-1) Europe (Ireland) (eu-west-1) Europe (Paris) (eu-west-3)
Australia	Asia Pacific (Tokyo) (ap-northeast-1) Asia Pacific (Seoul) (ap-northeast-2) Asia Pacific (Osaka) (ap-northeast-3) Asia Pacific (Mumbai) (ap-south-1) Asia Pacific (Singapore) (ap-southeast-1)

Supported Amazon Q Business geography	Inference regions
	Asia Pacific (Sydney) (ap-southeast-2)

Amazon Q Business Service improvement

Amazon Q Business does not use customer data for service improvement or for improving underlying LLMs.

Amazon Q Business and interface Amazon VPC endpoints (AWS PrivateLink)

You can establish a private connection between your Amazon VPC and Amazon Q Business by creating an interface VPC endpoint. Interface endpoints are powered by AWS PrivateLink, a technology that allows you to privately access Amazon Q Business APIs without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC don't need public IP addresses to communicate with Amazon Q Business APIs. Traffic between your VPC and Amazon Q Business doesn't leave the Amazon network.

Before you set up an interface VPC endpoint for Amazon Q Business, make sure that you review the prerequisites in the *Amazon VPC User Guide*.

Amazon Q Business currently only supports making API calls from your VPC for Amazon Q Business APIs only. Using your VPC for the web experience user interface is not supported.

Creating an interface VPC endpoint for Amazon Q Business

You can create an interface endpoint for Amazon Q Business using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI).

Create an interface endpoint for Amazon Q Business using the following service name:

```
aws.api.region.qbusiness
```

After you create a VPC endpoint, you can use the following example AWS CLI command that uses the `endpoint-url` parameter to specify an interface endpoint to the Amazon Q Business API:

```
aws qbusiness list-applications --endpoint-url https://VPC endpoint
```

VPC endpoint is the DNS name generated when the interface endpoint is created. This name includes the VPC endpoint ID and the Amazon Q Business service name, which includes the region. For example, `vpce-1234-adbcdef-us-west-2a.qbusiness.us-west-2.vpce.amazonaws.com`.

If you enable private DNS for the endpoint, you can make API requests to Amazon Q Business using its default DNS name for the region. For example, `qbusiness.us-west-2.api.aws`.

For more information, see Creating an interface endpoint in the *Amazon VPC User Guide*.

Creating a VPC endpoint policy for Amazon Q Business

An endpoint policy is an IAM resource that you can attach to an interface endpoint. The default endpoint policy allows full access to Amazon Q Business through the interface endpoint. To control the access allowed to Amazon Q Business from your VPC, attach a custom endpoint policy to the interface endpoint.

An endpoint policy specifies the following information:

- The principals/authorized users who can perform actions (AWS accounts, IAM users, and IAM roles)
- The actions that can be performed
- The resources on which the actions can be performed.

For more information, see Controlling access to services with VPC endpoints in the *Amazon VPC User Guide*.

Example: VPC endpoint policy for Amazon Q Business actions

The following is an example of an endpoint policy for Amazon Q Business. When attached to an endpoint, this policy grants access to all available Amazon Q Business actions for all principals/authorized users on all resources.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "qbusiness:*"
```

```
        ],
        "Resource":"*"
      }
   ]
}
```

Identity and access management for Amazon Q Business

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Amazon Q resources. IAM is an AWS service that you can use with no additional charge.

Topics

- Audience
- Authenticating with identities
- Managing access using policies
- How Amazon Q Business works with IAM
- Identity-based policy examples for Amazon Q Business
- AWS managed policies for Amazon Q Business
- AWS managed policies for Amazon Q Apps
- Using service-linked roles for Amazon Q Business
- Using service-linked roles for Amazon Q Apps
- Troubleshooting Amazon Q Business identity and access

Audience

How you use AWS Identity and Access Management (IAM) differs based on your role:

- **Service user** - request permissions from your administrator if you cannot access features (see Troubleshooting Amazon Q Business identity and access)
- **Service administrator** - determine user access and submit permission requests (see How Amazon Q Business works with IAM)
- **IAM administrator** - write policies to manage access (see Identity-based policy examples for Amazon Q Business)

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be authenticated as the AWS account root user, an IAM user, or by assuming an IAM role.

You can sign in as a federated identity using credentials from an identity source like AWS IAM Identity Center (IAM Identity Center), single sign-on authentication, or Google/Facebook credentials. For more information about signing in, see How to sign in to your AWS account in the *AWS Sign-In User Guide*.

For programmatic access, AWS provides an SDK and CLI to cryptographically sign requests. For more information, see AWS Signature Version 4 for API requests in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity called the AWS account *root user* that has complete access to all AWS services and resources. We strongly recommend that you don't use the root user for everyday tasks. For tasks that require root user credentials, see Tasks that require root user credentials in the *IAM User Guide*.

Federated identity

As a best practice, require human users to use federation with an identity provider to access AWS services using temporary credentials.

A *federated identity* is a user from your enterprise directory, web identity provider, or Directory Service that accesses AWS services using credentials from an identity source. Federated identities assume roles that provide temporary credentials.

For centralized access management, we recommend AWS IAM Identity Center. For more information, see What is IAM Identity Center? in the *AWS IAM Identity Center User Guide*.

IAM users and groups

An *IAM user* is an identity with specific permissions for a single person or application. We recommend using temporary credentials instead of IAM users with long-term credentials. For more information, see Require human users to use federation with an identity provider to access AWS using temporary credentials in the *IAM User Guide*.

An *IAM group* specifies a collection of IAM users and makes permissions easier to manage for large sets of users. For more information, see Use cases for IAM users in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity with specific permissions that provides temporary credentials. You can assume a role by switching from a user to an IAM role (console) or by calling an AWS CLI or AWS API operation. For more information, see Methods to assume a role in the *IAM User Guide*.

IAM roles are useful for federated user access, temporary IAM user permissions, cross-account access, cross-service access, and applications running on Amazon EC2. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy defines permissions when associated with an identity or resource. AWS evaluates these policies when a principal makes a request. Most policies are stored in AWS as JSON documents. For more information about JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Using policies, administrators specify who has access to what by defining which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. An IAM administrator creates IAM policies and adds them to roles, which users can then assume. IAM policies define permissions regardless of the method used to perform the operation.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you attach to an identity (user, group, or role). These policies control what actions identities can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

Identity-based policies can be *inline policies* (embedded directly into a single identity) or *managed policies* (standalone policies attached to multiple identities). To learn how to choose between managed and inline policies, see Choose between managed policies and inline policies in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples include IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-

based policies, service administrators can use them to control access to a specific resource. You must specify a principal in a resource-based policy.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Other policy types

AWS supports additional policy types that can set the maximum permissions granted by more common policy types:

- **Permissions boundaries** – Set the maximum permissions that an identity-based policy can grant to an IAM entity. For more information, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – Specify the maximum permissions for an organization or organizational unit in AWS Organizations. For more information, see Service control policies in the *AWS Organizations User Guide*.
- **Resource control policies (RCPs)** – Set the maximum available permissions for resources in your accounts. For more information, see Resource control policies (RCPs) in the *AWS Organizations User Guide*.
- **Session policies** – Advanced policies passed as a parameter when creating a temporary session for a role or federated user. For more information, see Session policies in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

How Amazon Q Business works with IAM

Before you use IAM to manage access to Amazon Q, learn what IAM features are available to use with Amazon Q.

IAM features you can use with Amazon Q Business

IAM feature	Amazon Q Business support
Identity-based policies	Yes
Resource-based policies	No
Policy actions	Yes
Policy resources	Yes
Policy condition keys	Yes
ACLs	No
ABAC (tags in policies)	Yes
Temporary credentials	Yes
Principal permissions	Yes
Service roles	Yes
Service-linked roles	Partial

To get a high-level view of how Amazon Q Business and other AWS services work with most IAM features, see AWS services that work with IAM in the *IAM User Guide*.

Identity-based policies for Amazon Q Business

Supports identity-based policies: Yes

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. To learn about all of the elements that you can use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

Identity-based policy examples for Amazon Q Business

To view examples of Amazon Q identity-based policies, see Identity-based policy examples for Amazon Q Business.

Resource-based policies within Amazon Q Business

Supports resource-based policies: No

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Policy actions for Amazon Q Business

Supports policy actions: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Include actions in a policy to grant permissions to perform the associated operation.

To see a list of Amazon Q Business actions, see Actions Defined by Amazon Q Business in the *Service Authorization Reference*.

Policy actions in Amazon Q Business use the following prefix before the action:

```
qbusiness
```

Policy actions in Amazon Q Business use the following prefix before the action: `qbusiness:`. For example, to grant someone permission to list an Amazon Q application with the `ListApplications` API operation, you include the `qbusiness:ListIndices` action in their policy. Policy statements must include either an `Action` or `NotAction` element. Amazon Q defines its own set of actions that describe tasks that you can perform with this service.

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [
      "qbusiness:action1",
      "qbusiness:action2"
         ]
```

To view examples of Amazon Q identity-based policies, see Identity-based policy examples for Amazon Q Business.

Policy resources for Amazon Q Business

Supports policy resources: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. As a best practice, specify a resource using its Amazon Resource Name (ARN). For actions that don't support resource-level permissions, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

To view examples of Amazon Q identity-based policies, see Identity-based policy examples for Amazon Q Business.

Policy condition keys for Amazon Q Business

Supports service-specific policy condition keys: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element specifies when statements execute based on defined criteria. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

To see a list of Amazon Q Business condition keys, see Condition Keys for Amazon Q Business in the *Service Authorization Reference*. To learn with which actions and resources you can use a condition key, see Actions Defined by Amazon Q Business .

To view examples of Amazon Q identity-based policies, see Identity-based policy examples for Amazon Q Business.

ACLs in Amazon Q Business

Supports ACLs: No

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

ABAC with Amazon Q

Supports ABAC (tags in policies): Yes

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes called tags. You can attach tags to IAM entities and AWS resources, then design ABAC policies to allow operations when the principal's tag matches the tag on the resource.

To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see Define permissions with ABAC authorization in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see Use attribute-based access control (ABAC) in the *IAM User Guide*.

The following table lists the actions, corresponding resource types, and condition keys for tag-based access control. Each action is authorized based on the tags associated with the corresponding resource type.

Action	Resource type	Condition keys
CreateApplication		aws:ResourceTag , aws:RequestTag , aws:TagKeys
CreateDataSource		aws:ResourceTag , aws:RequestTag , aws:TagKeys
CreateIndex		aws:ResourceTag , aws:RequestTag , aws:TagKeys
CreatePlugin		aws:ResourceTag , aws:RequestTag , aws:TagKeys
CreateRetriever		aws:ResourceTag , aws:RequestTag , aws:TagKeys
CreateWebExperience		aws:ResourceTag , aws:RequestTag , aws:TagKeys
ListTagsForResource	application, index, retriever, data source, web experience, plugin	
TagResource	application, index, retriever, data source, web experience, plugin	aws:ResourceTag , aws:RequestTag , aws:TagKeys

Action	Resource type	Condition keys
UntagResource	application, index, retriever, data source, web experience, plugin	aws:TagKeys

Using temporary credentials with Amazon Q Business

Supports temporary credentials: Yes

Temporary credentials provide short-term access to AWS resources and are automatically created when you use federation or switch roles. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM and AWS services that work with IAM in the *IAM User Guide*.

Cross-service principal permissions for Amazon Q Business

Supports forward access sessions (FAS): Yes

Forward access sessions (FAS) use the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. For policy details when making FAS requests, see Forward access sessions.

Service roles for Amazon Q

Supports service roles: Yes

A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Create a role to delegate permissions to an AWS service in the *IAM User Guide*.

> **Warning**
>
> Changing the permissions for a service role might break Amazon Q Business functionality. Edit service roles only when Amazon Q Business provides guidance to do so.

Service-linked roles for Amazon Q Business

Supports service-linked roles: Partial

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about creating or managing Amazon Q Business service-linked roles, see Using service-linked roles for Amazon Q Business.

For details about creating or managing service-linked roles, see AWS services that work with IAM. Find a service in the table that includes a `Yes` in the **Service-linked role** column. Choose the **Yes** link to view the service-linked role documentation for that service.

Identity-based policy examples for Amazon Q Business

By default, users and roles don't have permission to create or modify Amazon Q resources. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see Create IAM policies (console) in the *IAM User Guide*.

For details about actions and resource types defined by Amazon Q, including the format of the ARNs for each of the resource types, see Actions, Resources, and Condition Keys for Amazon Q Business in the *Service Authorization Reference*.

Topics

- Policy best practices
- Using the Amazon Q console
- Allow users to view their own permissions
- Allow a user to converse with Amazon Q Business
- Allow an admin to manage plugins in an application
- Allow an admin to manage a specific plugin
- Tag-based policy examples

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Amazon Q resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see Validate policies with IAM Access Analyzer in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Secure API access with MFA in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM in the *IAM User Guide*.

Using the Amazon Q console

To access the Amazon Q Business console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Amazon Q resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (users or roles) with that policy.

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that they're trying to perform.

To ensure that users and roles can still use the Amazon Q Business console, also attach the *ReadOnlyAcess*AWS managed policy to the entities. For more information, see Adding permissions to a user in the *IAM User Guide*.

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
```

```
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow a user to converse with Amazon Q Business

This example allows a user to start conversations with Amazon Q Business, view past conversations, and delete their conversation history for a specific Amazon Q Business application. The IAM context key *qbusiness:userId* is used to restrict permissions to a specific user.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "qbusiness:ChatSync",
                "qbusiness:ListMessages",
                "qbusiness:ListConversations",
                "qbusiness:GetWebExperience",
                "qbusiness:DeleteConversation",
                "qbusiness:GetMedia"
            ],
            "Resource": [
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
            ],
            "Effect": "Allow",
            "Sid": "QBusinessChatPermissions"
        }
    ]
}
```

Allow an admin to manage plugins in an application

This example allows an Amazon Q Business admin to manage plugins in a chat application.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "qbusiness:CreatePlugin",
                "qbusiness:ListPlugins",
                "qbusiness:GetPlugin",
                "qbusiness:UpdatePlugin",
                "qbusiness:DeletePlugin"
            ],
            "Resource": [
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
            ],
            "Effect": "Allow",
            "Sid": "QBusinessListPermissions"
        }
    ]
}
```

Allow an admin to manage a specific plugin

This example allows an Amazon Q Business admin to manage a specific plugin.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "qbusiness:GetPlugin",
                "qbusiness:UpdatePlugin",
```

```
                "qbusiness:DeletePlugin"
            ],
            "Resource": [
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id",
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id/plugin/plugin-id"
            ],
            "Effect": "Allow",
            "Sid": "QBusinessGetPermissions"
        }
    ]
}
```

Tag-based policy examples

Tag-based policies are JSON policy documents that specify the actions that a principal can perform on tagged resources.

Example: Use a tag to access a resource

This example policy grants a user or role in your AWS account permission to use the `ChatSync` operation with any resource tagged with the key **`department`** and the value **`finance`**.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "qbusiness:ChatSync"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/department": "finance"
                }
```

```
            },
            "Sid": "QBusinessChatPermissions"
        }
    ]
}
```

Example: Use a tag to activate operations

This example policy grants a user or role in your AWS account permission to use any Amazon Q Business operation except the `TagResource` operation with any resource tagged with the key **`department`** and the value **`finance`**.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessFullAccessPermissions",
            "Effect": "Allow",
            "Action": "qbusiness:*",
            "Resource": "*"
        },
        {
            "Sid": "QBusinessPermissions",
            "Effect": "Deny",
            "Action": [
                "qbusiness:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/department": "finance"
                }
            }
        }
    ]
}
```

Example: Use a tag to restrict access to an operation

This example policy restricts access for a user or role in your AWS account to use the `ChatSync` operation unless the user provides the **`department`** tag and it has the allowed values **`finance`** and **`IT`**.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": "qbusiness:ChatSync",
            "Resource": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id",
            "Effect": "Allow",
            "Sid": "QBusinessChatSyncPermissions"
        },
        {
            "Action": "qbusiness:ChatSync",
            "Resource": "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id",
            "Effect": "Deny",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/department": "true"
                }
            },
            "Sid": "DenyChatSyncWithoutDepartmentTag"
        },
        {
            "Action": "qbusiness:ChatSync",
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:ResourceTag/department": [
                        "finance",
                        "IT"
                    ]
                }
            },
```

```
            "Sid": "DenyChatSyncForUnauthorizedDepts"
        }
    ]
}
```

AWS managed policies for Amazon Q Business

An AWS managed policy is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases so that you can start assigning permissions to users, groups, and roles.

Keep in mind that AWS managed policies might not grant least-privilege permissions for your specific use cases because they're available for all AWS customers to use. We recommend that you reduce permissions further by defining customer managed policies that are specific to your use cases.

You cannot change the permissions defined in AWS managed policies. If AWS updates the permissions defined in an AWS managed policy, the update affects all principal identities (users, groups, and roles) that the policy is attached to. AWS is most likely to update an AWS managed policy when a new AWS service is launched or new API operations become available for existing services.

For more information, see AWS managed policies in the *IAM User Guide*.

Topics

- AWS managed policy: QBusinessServiceRolePolicy
- AWS managed policy: QBusinessQuicksightPluginPolicy
- Amazon Q Business updates to AWS managed policies

AWS managed policy: QBusinessServiceRolePolicy

Amazon Q Business uses a `QBusinessServiceRolePolicy` to enable an Amazon Q Business application to access CloudWatch resources and write CloudWatch logs. You can't attach `QBusinessServiceRolePolicy` to your IAM entities. This policy is attached to a service-linked role that allows Amazon Q Business to perform actions on your behalf. For more information, see Using service-linked roles for Amazon Q Business.

Permissions details

This policy includes the following permissions.

- `logs` – Allows Amazon Q Business to describe and write to CloudWatch log streams.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessPutMetricDataPermission",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/QBusiness"
                }
            }
        },
        {
            "Sid": "QBusinessCreateLogGroupPermission",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/qbusiness/*"
            ],
```

```
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "QBusinessDescribeLogGroupsPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "QBusinessLogStreamPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogStreams",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/qbusiness/*:log-stream:*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
    ]
}
```

AWS managed policy: QBusinessQuicksightPluginPolicy

Amazon Q Business uses a `QBusinessQuicksightPluginPolicy` to enable an Amazon Q Business application to access Amazon Quick topics and dashboards for the Amazon Q Business Quick plugin. When you configure the plugin, you specify a service role that has `PredictQAResults` permissions for Quick topics and dashboards. You can use the following `QBusinessQuicksightPluginPolicy` policy to grant these permissions.

> **Note**
>
> To grant the necessary permissions, the trust policy of the role must grant Quick assume role permissions. For more information see Using the Quick plugin to get insights from structured data.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "QBusinessToQuickSightPredictQAResultsInvocation",
      "Effect": "Allow",
      "Action": [
        "quicksight:PredictQAResults"
      ],
      "Resource": [
        "arn:aws:quicksight:*:*:topic/*",
        "arn:aws:quicksight:*:*:dashboard/*"
      ]
    }
  ]
}
```

Amazon Q Business updates to AWS managed policies

View details about updates to AWS managed policies for Amazon Q Business since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Amazon Q Business Document history page.

Change	Description	Date
AWS managed policy: QBusinessQuicksightPluginPolicy	Added AWS managed policy QBusinessQuicksightPluginPolicy to access Amazon Quick resources for the QuickSight plugin.	December 3, 2024
Amazon Q Business started tracking changes	Amazon Q Business started tracking changes for its AWS managed policies.	April 30, 2024

AWS managed policies for Amazon Q Apps

An AWS managed policy is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases so that you can start assigning permissions to users, groups, and roles.

Keep in mind that AWS managed policies might not grant least-privilege permissions for your specific use cases because they're available for all AWS customers to use. We recommend that you reduce permissions further by defining customer managed policies that are specific to your use cases.

You cannot change the permissions defined in AWS managed policies. If AWS updates the permissions defined in an AWS managed policy, the update affects all principal identities (users, groups, and roles) that the policy is attached to. AWS is most likely to update an AWS managed policy when a new AWS service is launched or new API operations become available for existing services.

For more information, see AWS managed policies in the *IAM User Guide*.

AWS managed policy: QAppsServiceRolePolicy

Amazon Q Apps uses a `QAppsServiceRolePolicy` to enable an Amazon Q Apps to access CloudWatch resources and populate CloudWatch metrics. You can't attach `QAppsServiceRolePolicy` to your IAM entities. This policy is attached to a service-linked role that allows Amazon Q Apps to perform actions on your behalf. For more information, see Using service-linked roles for Amazon Q Apps.

Permissions details

This policy includes the following permissions.

- `cloudwatch` – Allows Amazon Q Apps to publish metric data points to CloudWatch under the AWS/QApps namespace

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QAppsPutMetricDataPermission",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/QApps"
                }
            }
        }
    ]
```

```
}
```

Amazon Q Apps updates to AWS managed policies

View details about updates to AWS managed policies for Amazon Q Apps since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Amazon Q Business Document history page.

Change	Description	Date
QAppsServiceRolePolicy - New policy	Amazon Q Apps added a new policy that grants permissions needed for Q Apps to publish metrics	Sep 30, 2024
Amazon Q Apps started tracking changes	Amazon Q Apps started tracking changes for its AWS managed policies.	Sep 30, 2024

Using service-linked roles for Amazon Q Business

Amazon Q Business uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Amazon Q Business. Service-linked roles are predefined by Amazon Q Business and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Amazon Q Business easier because you don’t have to manually add the necessary permissions. Amazon Q Business defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon Q Business can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting their related resources. This protects your Amazon Q Business resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-linked roles** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Amazon Q Business

Amazon Q Business uses one service-linked role named `AWSServiceRoleForQBusiness` that performs certain actions in your account. Examples of these actions include allowing CloudWatch to publish metrics and logs to your AWS account.

QBusinessServiceRolePolicy permissions details

The `QBusinessServiceRolePolicy` allows Amazon Q Business to complete the following administrative actions on the user's behalf on all applicable AWS resources:

- `logs` – Allows Amazon Q Business to describe, create and write to CloudWatch log streams
- `cloudwatch` – Allows Amazon Q Business to publish metric data points to CloudWatch under the AWS/QBusiness namespace

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "QBusinessPutMetricDataPermission",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/QBusiness"
                }
            }
        },
        {
            "Sid": "QBusinessCreateLogGroupPermission",
            "Effect": "Allow",
            "Action": [
```

```
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/qbusiness/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "QBusinessDescribeLogGroupsPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "QBusinessLogStreamPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogStreams",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/qbusiness/*:log-stream:*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
    ]
}
```

Any updates to this policy are described in Amazon Q Business updates to AWS managed policies.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the IAM User Guide.

Creating a service-linked role for Amazon Q Business

You don't need to manually create a service-linked role. When you create an Amazon Q Business application in the AWS Management Console, the AWS CLI, or the AWS API, Amazon Q Business creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create a new application, Amazon Q Business creates the service-linked role for you again.

You can also use the IAM console to create a service-linked role. In the IAM CLI or the IAM API, create a service-linked role with the `qbusiness.amazonaws.com` service name. For more information, see Creating a service-linked role in the IAM User Guide. If you delete this service-linked role, you can use this same process to create the role again.

You can also choose to create an Amazon Q Business application with a service role instead of a service-linked role. However, using a service-linked role is recommended.

For Amazon Q Business applications created before April 2024

If your Amazon Q Business application was created before April 2024, it uses a service role instead of a service-linked role.

To migrate your existing application from a service role to a service-linked role, create a service-linked role with the `qbusiness.amazonaws.com` service name. Then, if you use the console, select to use the newly created service-linked role when you update your application. If you use the API, provide the ARN of the service-linked role as the `roleArn` parameter when you use the UpdateApplication API action.

For more information, see Creating a service-linked role in the IAM User Guide.

Editing a service-linked role for Amazon Q Business

Amazon Q Business does not allow you to edit service-linked roles. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role.

However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the *IAM User Guide*.

Changing between a service-role and a service-linked role for Amazon Q Business

You can choose to update the service-linked role you are using when you update an application.

For an application using a service role, you can update the role to a service-linked role.

For an application already using a service-linked role, you can update the role to a service role.

You can also choose to continue using a service role, or update an existing service role with a new one.

> **Note**
>
> Using a service-linked role is recommended.

For more information on how to update your application, see Updating an application.

Deleting a service-linked role for Amazon Q Business

You can manually delete your `AWSServiceRoleForQBusiness` role. If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must delete your application before you can manually delete the service-linked role associated with it.

> **Note**
>
> If the Amazon Q Business service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To manually delete the service-linked role using IAM

Use the IAM console, the IAM CLI, or the IAM API to delete the `AWSServiceRoleForQBusiness` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported regions for Amazon Q Business service-linked roles

Amazon Q Business supports using service-linked roles in all of the regions where the service is available. For more information, see Amazon Q Business endpoints and quotas.

Using service-linked roles for Amazon Q Apps

Amazon Q Apps uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Amazon Q Apps. Service-linked roles are predefined by Amazon Q Apps and include all the permissions that the service requires to performs Q Apps related administrative actions to other AWS services on your behalf.

A service-linked role makes setting up Amazon Q Apps easier because you don't have to manually add the necessary permissions. Amazon Q Apps defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon Q Apps can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting their related resources. This protects your Amazon Q Apps resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-linked roles** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Amazon Q Apps

Amazon Q Apps uses one service-linked role named `AWSServiceRoleForAmazonQApps` that performs Q Apps related administrative actions in your account. Examples of these actions include allowing CloudWatch to publish metrics to your AWS account.

The `AWSServiceRoleForAmazonQApps` service-linked role trusts the following services to assume the role:

- qapps.amazonaws.com

The `AWSServiceRoleForAmazonQApps` service-linked role uses the managed policy `QAppsServiceRolePolicy`.

The content of this policy and any updates to it are described in AWS managed policies for Amazon Q Apps.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the IAM User Guide.

Creating a service-linked role for Amazon Q Apps

You don't need to manually create a service-linked role. When you create an Amazon Q Business application in the AWS Management Console, the AWS CLI, or the AWS API, Amazon Q Apps creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create a new application, Amazon Q Apps creates the service-linked role for you again.

Editing a service-linked role for Amazon Q Apps

Amazon Q Apps does not allow you to edit service-linked roles. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the *IAM User Guide*.

Deleting a service-linked role for Amazon Q Apps

You can manually delete your `AWSServiceRoleForQApps` role. If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don’t have an unused entity that is not actively monitored or maintained. However, you must delete your Q application or turn on QApps on all existing Q applications before you can manually delete the service-linked role associated with it.

> **Note**
>
> If the Amazon Q Apps service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To manually delete the service-linked role using IAM

Use the IAM console, the IAM CLI, or the IAM API to delete the `AWSServiceRoleForQApps` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported regions for Amazon Q Apps service-linked roles

Amazon Q Apps supports using service-linked roles in all of the regions where the service is available. For more information, see Amazon Q Business endpoints and quotas.

Troubleshooting Amazon Q Business identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon Q and IAM.

Topics

- I am not authorized to perform an action in Amazon Q Business
- I am not authorized to perform iam:PassRole
- I want to allow people outside of my AWS account to access my Amazon Q Business resources

I am not authorized to perform an action in Amazon Q Business

If you receive an error that you're not authorized to perform an action, your policies must be updated to allow you to perform the action.

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a fictional *`my-example-widget`* resource but doesn't have the fictional `qbusiness:`*`GetWidget`* permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 qbusiness:GetWidget on resource: my-example-widget
```

In this case, the policy for the `mateojackson` user must be updated to allow access to the *`my-example-widget`* resource by using the `qbusiness:`*`GetWidget`* action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to Amazon Q.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Amazon Q. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to allow people outside of my AWS account to access my Amazon Q Business resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon Q supports these features, see How Amazon Q Business works with IAM.
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.

Compliance validation for Amazon Q Business

Third-party auditors assess the security and compliance of Amazon Q Business as part of multiple Amazon Q Business compliance programs. Amazon Q Business is compliant with the following:

- Health Insurance Portability and Accountability Act (HIPAA)
- System and Organization Controls (SOC) 1, 2, 3
- Payment Card Industry (PCI)
- International Standards Organization (ISO) 42001

To learn whether an AWS service is within the scope of specific compliance programs, see AWS services in Scope by Compliance Program and choose the compliance program that you are interested in. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. For more information about your compliance responsibility when using AWS services, see AWS Security Documentation.

Using ACL Analyzer in Amazon Q

The ACL (Access Control List) Analyzer is a troubleshooting tool that helps you verify and diagnose document access permissions in your Amazon Q applications. When users report issues accessing specific documents, you can use this tool to quickly determine whether a user has the necessary permissions and understand why access might be granted or denied. The tool provides detailed information about user memberships, group associations, and the specific access control rules affecting document accessibility. This makes it particularly useful for administrators who need to validate access controls or investigate permission-related issues.

Prerequisites

- An AWS account with appropriate permissions for Amazon Q Business
- Access to the Amazon Q Business service in the AWS Console

Getting Started with ACL Analyzer

To access Amazon Q Business

1. Sign in to the AWS Management Console.
2. Open the Amazon Q Business console.

To select or create an application:

1. In the navigation pane, choose **Applications**.
2. Do one of the following:
   - Choose an existing application from the list.
   - Create a new application.

> **Note**
>
> The application you select or create will be used as the context for checking document access permissions.

To configure user access

1. On the application details page, choose **Manage access and subscriptions**.
2. Choose the **Users** tab.
3. Choose **Add groups and users**.
4. Do one of the following:
5. a. To add new users:

   Choose **Add new users**.

   b. Enter the required user information.

   c. Choose **Done**.
6. a. To assign existing users:

   Choose **Assign existing users**.

   b. Search for and select the desired user.

c. Choose **Assign**.

Configuring Data Sources

To configure a new data source

1. On the application details page, choose **Add data source**.
2. Select your desired data source type from the available options.
3. Follow the configuration prompts specific to your selected data source type.
4. Configure the ACL settings for your data source. For detailed instructions, see:

   - Setting up data sources
   - Managing user access

To use an existing data source

1. On the application details page, choose **Data sources**.
2. From the list of data sources, select the data source you want to use.

Using the ACL Analyzer Tool

To check document access permissions

1. On the data source details page, choose the **Troubleshooting tools** tab.
2. Locate the **ACL Analyzer** section.
3. Enter the following required information:

   - For **Document ID**, enter the unique identifier of the document you want to check.

     > **Note**
     >
     > The Document ID must conform to the pattern specified in the API documentation.

   - For **User ID**, enter the ID of the user whose access you want to verify, typically this is an email address.
4. Choose **Check access**.

Understanding the Results

After running the ACL Analyzer check, you'll see results in three main sections:

Access Status

The system displays one of the following status messages:

- A success message indicating "**User has access**" when access is granted.
- An error message indicating "**User doesn't have access**" when access is denied.

User Membership Table

This table provides the following information:

- All user aliases associated with the checked user ID.
- User or group mapping information.
- Source configurations for each membership. Datasource level ACL applies only to the datasource and index level ACL applies to the entire index/application.

Access Control List (ACL) Table

This table shows:

- The allowlist of Users/Groups with access to the specified document, as defined by documentId.

Resilience in Amazon Q Business

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

Infrastructure security in Amazon Q Business

As a managed service, Amazon Q Business is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see AWS Cloud Security. To design your AWS environment using the best practices for infrastructure security, see Infrastructure Protection in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access Amazon Q through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Cross-service confused deputy prevention

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access. To prevent this, AWS provides tools that help you protect your data for all services with service principals that have been given access to resources in your account.

We recommend using the aws:SourceArn global condition context key in resource policies to limit the permissions that Amazon Q Business gives another service to the resource.

The value of `aws:SourceArn` must be `qbusiness::Application`.

The following example—which grants Amazon Q Business permission to perform a decryption action on an AWS KMS key within the scope of an Amazon Q Business application—shows how you can use the `aws:SourceArn` global condition context key in Amazon Q Business to prevent the confused deputy problem.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Sid": "ConfusedDeputyPreventionExamplePolicy",
        "Effect": "Allow",
        "Principal": {
            "Service": "qbusiness.amazonaws.com"
        },
        "Action": "kms:Decrypt",
        "Resource": [
            "arn:aws:qbusiness:us-east-1:111122223333:application/application-id/
*"
        ],
        "Condition": {
            "ArnLike": {
                "aws:SourceArn": "arn:aws:qbusiness:us-
east-1:111122223333:application/*"
            }
        }
    }
}
```

Configuration and vulnerability analysis in AWS Identity and Access Management

AWS handles basic security tasks like guest operating system (OS) and database patching, firewall configuration, and disaster recovery. These procedures have been reviewed and certified by the appropriate third parties. For more details, see the following resources:

- Shared Responsibility Model
- AWS: Overview of Security Processes (whitepaper)

The following resources also address configuration and vulnerability analysis in AWS Identity and Access Management (IAM):

- Compliance validation for AWS Identity and Access Management

- Security best practices and use cases in AWS Identity and Access Management.

Security best practices

Amazon Q Business provides several security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don't represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.

Apply principle of least privilege

Amazon Q provides a granular access policy for applications using IAM roles. We recommend that the roles be granted only the minimum set of privileges required by the job, such as covering your application and access to log destination. We also recommend auditing the jobs for permissions on a regular basis and upon any change to your application.

Role-based access control (RBAC) permissions

Administrators should strictly control role-based access control (RBAC) permissions for Amazon Q applications.

Monitoring Amazon Q Business and Q Apps

Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon Q Business and your other AWS solutions. AWS provides the following monitoring tools to monitor Amazon Q Business, report when something is wrong, and take automatic actions when appropriate:

- *AWS CloudTrail* captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the AWS CloudTrail User Guide.
- *Amazon CloudWatch* monitors your AWS resources and the applications you run on AWS in real time. You can collect and track metrics, create customized dashboards, and set alarms that notify you or take actions when a specified metric reaches a threshold that you specify. For example, you can have CloudWatch track CPU usage or other metrics of your Amazon EC2 instances and automatically launch new instances when needed. For more information, see the Amazon CloudWatch User Guide.
- You can use Amazon CloudWatch Logs to monitor and analyze user conversations and response feedback in Amazon Q Business. CloudWatch Logs can deliver logs to multiple locations, such as Amazon CloudWatch, Amazon S3, or Amazon Data Firehose (standard rates apply). We recommend that you set up conversation and feedback logging with Amazon CloudWatch within five minutes of creating your Amazon Q Business Application environment. For more information, see Monitoring Amazon Q Business user conversations with Amazon CloudWatch Logs.

Topics

- Logging Amazon Q Business API calls using AWS CloudTrail
- Logging Amazon Q Apps API calls using AWS CloudTrail
- Monitoring Amazon Q Business and Amazon Q Apps with Amazon CloudWatch
- Monitoring Amazon Q Business user conversations with Amazon CloudWatch Logs
- Viewing Amazon Q Business and Q App metrics in analytics dashboards

Logging Amazon Q Business API calls using AWS CloudTrail

Amazon Q Business is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon Q Business. CloudTrail captures all API calls for Amazon Q Business as events. The calls captured include calls from the Amazon Q console and code calls to the Amazon Q Business API operations. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon Q Business. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to Amazon Q Business, the IP address from which the request was made, who made the request, when it was made, and additional details.

For more information about CloudTrail, including how to configure and activate it, see the AWS CloudTrail User Guide.

Amazon Q Business information in CloudTrail

CloudTrail is activated on your AWS account when you create the account. When activity occurs in Amazon Q Business, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing events with CloudTrail Event history in the *AWS CloudTrail User Guide*.

For an ongoing record of events in your AWS account, including events for Amazon Q, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following topics:

- Creating a trail for your AWS account
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple Regions and Receiving CloudTrail log files from multiple accounts

Control plane events in CloudTrail

CloudTrail supports logging the following Amazon Q Business actions documented in the Amazon Q Business API Reference:

- CreateApplication
- DeleteApplication
- GetApplication
- ListApplications
- UpdateApplication
- DeleteChatControlsConfiguration
- GetChatControlsConfiguration
- UpdateChatControlsConfiguration
- CreateDataSource
- DeleteDataSource
- GetDataSource
- ListDataSources
- UpdateDataSource
- CreateWebExperience
- DeleteWebExperience
- ListWebExperiences
- UpdateWebExperience
- CreateIndex
- DeleteIndex
- GetIndex
- ListIndices
- UpdateIndex
- CreatePlugin
- DeletePlugin
- GetPlugin
- ListPlugins
- UpdatePlugin

- CreateRetriever
- DeleteRetriever
- GetRetriever
- ListRetrievers
- UpdateRetriever
- ListTagsForResource
- TagResource
- UntagResource

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see CloudTrail userIdentity element in the *AWS CloudTrail User Guide*.

Data plane events in CloudTrail

Data events provide information about the resource operations performed on or in a resource (for example, reading or writing to an Amazon S3 object). These are also known as *data plane operations*. By default, CloudTrail doesn't log data events.

The following table shows the Amazon Q Business API operations logged to CloudTrail as *data events*. The **Data event type (console)** column shows the appropriate selection in the CloudTrail console. The **Amazon Q Business resource types** column shows the `resources.type` value that you would specify to log data events for the resource.

Data event type (console)	Amazon Q Business resource types	Supported data events
Amazon Q Business application	`AWS::QBusiness::Application`	• ListDataSourceSyncJobs • StartDataSourceSyncJob

Data event type (console)	Amazon Q Business resource types	Supported data events
		• StopDataSourceSyncJob • BatchPutDocument • BatchDeleteDocument • PutFeedback • ChatSync • Chat • DeleteConversation • ListConversations • ListMessages • ListGroups • DeleteGroup • GetGroup • PutGroup • CreateUser • DeleteUser • GetUser • UpdateUser • ListDocuments
Amazon Q Business data resource	`AWS::QBusiness::DataSource`	• ListDataSourceSyncJobs • StartDataSourceSyncJob • StopDataSourceSyncJob

Data event type (console)	Amazon Q Business resource types	Supported data events
Amazon Q Business index	`AWS::QBusiness::Index`	• DeleteGroup • GetGroup • PutGroup • ListGroups • ListDocuments • BatchPutDocument • BatchDeleteDocument

You can log these API operations by configuring advanced event selectors to record data events for the Amazon Q Business resource types: `AWS::QBusiness::Application`, `AWS::QBusiness::DataSource`, and `AWS::QBusiness::Index`. To configure advanced event selectors, you can use either the CloudTrail console or the AWS CLI:

- From the CloudTrail console, choose the **Data event type** for which you want to log data events. Additionally, you can filter on the `eventName` and `resources.ARN` fields by choosing a custom log selector template. For more information, see Logging data events with the AWS Management Console in the *AWS CloudTrail User Guide*.
- From the AWS CLI, specify the `resources.type` value for which you want to log data events and set the `eventCategory` equal to `Data`. For more information, see Logging data events with the AWS CLI in the *AWS CloudTrail User Guide*.

  The following example shows how to configure a trail to log all Amazon Q Business data events for all Amazon Q Business resource types.

```
aws cloudtrail put-event-selectors --trail-name trailName \
--advanced-event-selectors \
'[
  {
    "Name": "Log all data events on an Amazon Q Business application",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::QBusiness::Application"] }
    ]
  },
```

```
  {
    "Name": "Log all data events on an Amazon Q Business data source",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::QBusiness::DataSource"] }
    ]
  },
  {
    "Name": "Log all data events on an Amazon Q Business index",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::QBusiness::Index"] }
    ]
  }
]'
```

You can additionally filter on the `eventName` and `resources.ARN` fields. For more information about configuring these fields, see AdvancedFieldSelector in the *AWS CloudTrail API Reference*.

Additional charges apply for data events. For more information about CloudTrail pricing, see AWS CloudTrail Pricing.

Amazon Q Business management events in CloudTrail

Management events provide information about management operations that are performed on resources in your AWS account. These management events are also known as *control plane operations*. CloudTrail logs management event API operations by default.

Amazon Q Business logs the remainder of Amazon Q Business API operations as management events. For a list of the Amazon Q Business API operations that Amazon Q logs to CloudTrail, see the Amazon Q Business API Reference.

Understanding Amazon Q Business log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `CreateApplication` action.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principal ID",
        "arn": "ARN",
        "accountId": "account ID",
        "accessKeyId": "access key ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principal ID",
                "arn": "ARN",
                "accountId": "account ID",
                "userName": "user name"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "yyyy-mm-ddThh:mm:ssZ",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "yyyy-mm-ddThh:mm:ssZ",
    "eventSource": "qbusiness.amazonaws.com",
    "eventName": "CreateApplication",
    "awsRegion": "region",
    "sourceIPAddress": "region",
    "userAgent": "user agent",
    "requestParameters": {
        "name": "name",
        "roleArn": "description",
        "clientToken": "client token"
    },
    "responseElements": {
        "applicationId": "application ID"
    },
    "requestID": "request ID",
    "eventID": "event ID",
    "readOnly": false,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "account ID",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLS version",
        "cipherSuite":  "cipher suite",
        "clientProvidedHostHeader": "qbusiness.us-west-2.api.aws"
    }
}
```

Logging Amazon Q Apps API calls using AWS CloudTrail

Amazon Q Apps is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon Q Apps. CloudTrail captures all API calls for Amazon Q Apps as events. The calls captured include calls from theAmazon Q Apps web experience, console and code calls to theAmazon Q Apps API operations.

A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon Q Apps. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to Amazon Q Apps, the IP address from which the request was made, who made the request, when it was made, and additional details.

For more information about CloudTrail, including how to configure and activate it, see the *AWS CloudTrail User Guide*.

Amazon Q Apps information in CloudTrail

CloudTrail is activated on your AWS account when you create the account. When activity occurs in Amazon Q Apps, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history** in the CloudTrail console. You can view, search, and download recent events in your AWS account. For more information, see Viewing events with CloudTrail Event history in the *AWS CloudTrail User Guide*.

For an ongoing record of events in your AWS account, including events for Amazon Q Apps, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify.

Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following topics:

- Creating a trail for your AWS account
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple regions and Receiving CloudTrail log files from multiple accounts

Management events

Management events provide information about management operations that are performed on resources in your AWS account. These management events are also known as control plane operations. CloudTrail logs management event API operations by default.

CloudTrail supports logging the followingAmazon Q Apps actions:

- `CreateLibraryItem`
- `UpdateLibraryItem`
- `DeleteLibraryItem`
- `GetLibraryItem`
- `ListLibraryItems`
- `TagResource`
- `UntagResource`
- `ListTagsForResource`

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see CloudTrail userIdentity element in the *AWS CloudTrail User Guide*.

Data events

Data events provide visibility into the resource operations performed on or within a resource. These are also known as data plane operations. Data events are often high-volume activities. By default, CloudTrail doesn't log data events.

The following table shows theAmazon Q Apps API operations logged to CloudTrail as data events. The **Data event type (console)** column shows the appropriate selection in the CloudTrail console. The **Amazon Q Apps resource types column** shows the `resources.type` value that you would specify to log data events for the resource.

Data event type (console)	Amazon Q Apps resource types	Supported data events
Amazon Q Apps	`AWS::QApps::QApp`	• `CreateQApp` • `CopyQApp` • `UpdateQApp` • `DeleteQApp` • `AssociateQAppWithUser` • `DisassociateQAppFromUser` • `ImportDocumentToQApp` • `ImportDocumentToQAppSession` • `CreateLibraryItemReview` • `StartQAppSession` • `StopQAppSession` • `GetQApp` • `ListQApps` • `ImportDocument` • `GetQAppSession`

Data event type (console)	Amazon Q Apps resource types	Supported data events
		• UpdateQAppSession • AssociateLibraryItemReview • DisassociateLibraryItemReview
Amazon Q Business application	AWS::QBusiness::Application	• CreateSubscriptionToken • PredictProblemStatementFromConversation • PredictQAppFromProblemStatement • PredictQApp

You can log these API operations by configuring advanced event selectors to record data events for theAmazon Q Apps resource types: AWS::QApps::QApp and AWS::QBusiness::Application. To configure advanced event selectors, you can use either the CloudTrail console or the AWS CLI:

- From the CloudTrail console, choose the **Data event type** for which you want to log data events. Additionally, you can filter on the eventName and resources.ARN fields by choosing a custom log selector template. For more information, see Logging data events with the AWS Management Console in the *AWS CloudTrail User Guide*.
- From the AWS CLI, specify the resources.type value for which you want to log data events and set the eventCategory equal to Data. For more information, see Logging data events with the AWS CLI in the *AWS CloudTrail User Guide*. The following example shows how to configure a trail to log allAmazon Q Apps data events for allAmazon Q Apps resource types.

```
aws cloudtrail put-event-selectors --trail-name trailName \
--advanced-event-selectors \
'[
  {
```

```
    "Name": "Log all data events on anAmazon Q Apps",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::QApps::QApp"] }
    ]
  }
]'
```

You can additionally filter on the `eventName` and `resources.ARN` fields. For more information about configuring these fields, see AdvancedFieldSelector in the *AWS CloudTrail API Reference*.

> **Note**
>
> Additional charges apply for data events. For more information about CloudTrail pricing, see AWS CloudTrail Pricing.

UnderstandingAmazon Q Apps log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `GetLibraryItem` action.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principal ID",
        "arn": "ARN",
        "accountId": "account ID",
        "accessKeyId": "access key ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
```

```
                "principalId": "principal ID",
                "arn": "ARN",
                "accountId": "account ID",
                "userName": "user name"
            },
            "attributes": {
                "creationDate": "yyyy-mm-ddThh:mm:ssZ",
                "mfaAuthenticated": "false"
            }
        },
        "onBehalfOf": {
            "userId": "user ID",
            "identityStoreArn": "ARN"
        }
    },
    "eventTime": "yyyy-mm-ddThh:mm:ssZ",
    "eventSource": "qapps.amazonaws.com",
    "eventName": "GetLibraryItem",
    "awsRegion": "region",
    "sourceIPAddress": "source IP address",
    "userAgent": "user agent",
    "requestParameters": {
        "input": "query input",
        "idc-application-arn": "ARN",
        "application-id": "Q application ID"
    },
    "requestID": "request ID",
    "eventID": "event ID",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "account ID",
    "eventCategory": "Management"
}
```

Monitoring Amazon Q Business and Amazon Q Apps with Amazon CloudWatch

You can monitor Amazon Q Business and Amazon Q Apps with Amazon CloudWatch, which collects raw data and processes it into readable, near real-time metrics. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective on how your

web application or service is performing. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the Amazon CloudWatch User Guide.

Topics

- Using CloudWatch Metrics
- Viewing metrics
- Creating a CloudWatch alarm
- Amazon Q Business chat metrics
- Amazon Q Business API operation metrics
- Amazon Q Business index metrics
- Amazon Q Apps metrics

Using CloudWatch Metrics

To use metrics, you must specify the following information:

- The metric namespace. A *namespace* is a CloudWatch container Amazon Q uses to publish its metrics into. If you are using the CloudWatch ListMetrics API or the list-metrics command to view the metrics for Amazon Q Business or Amazon Q Apps, specify `AWS/QBusiness` or `AWS/QApps` for the namespace.
- The metric dimension. A *dimension* is a name-value pair that helps you to uniquely identify a metric. Common dimension names include:
  - `ApplicationId` - Identifies the specific Amazon Q Business application
  - `IndexId` - Identifies the specific index (for index-related metrics)
  - `DataSourceId` - Identifies the specific data source (for data source metrics)
  - `PluginId` - Identifies the specific plugin (for plugin-related metrics)
  - `API name` - Identifies the specific API operation (for performance metrics like Chat)
  - `MethodType` - Identifies the specific method being called (for API operation metrics)
  - `UsefulnessReason` - Identifies feedback categories (for feedback metrics)
- The metric name. For example, `DocumentsIndexed`.

You can get monitoring data for Amazon Q Business or Q Apps with the AWS Management Console, the AWS CLI, or the CloudWatch API. You can also use the CloudWatch API through one of the AWS SDKs or the CloudWatch API tools. The console displays a series of graphs based on the raw data from the CloudWatch API. Depending on your needs, you might prefer to use either the graphs displayed in the console or retrieved from the API.

The following table shows some common uses for the metrics. These are suggestions to get you started, not a comprehensive list.

How do I?	Relevant metrics
How do I track how many documents were indexed successfully?	Use the `DocumentsIndexed` metrics.
How do I monitor end user experience for Amazon Q Business?	Use the `ThumbsUpCount` and `ThumbsDownCount` metrics.
How do I track how many users used Q Apps	Use the `ActiveUsers` metric.
How do I track API operation success rates?	Use the `success` and `failure` metrics with appropriate `MethodType` dimensions.
How do I monitor individual API operation performance?	Use the `latency` metric with specific `MethodType` dimensions.
How do I monitor chat response performance and latency?	Use the `TimeToFirstToken` and `Latency` metrics with API name dimension set to "Chat".

You must have the appropriate CloudWatch permissions to monitor Amazon Q Business with CloudWatch. For more information, see Identity and access management for Amazon CloudWatch in the *Amazon CloudWatch User Guide*.

Viewing metrics

The following steps show how to access Amazon Q Business or Amazon Q Apps metrics using the CloudWatch console.

To view metrics (console)

1. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
2. Choose **Metrics**, choose the **All Metrics** tab, and then choose **AWS/QBusiness** or **AWS/QApps**.

> **Note**
>
> Some Q Apps metrics might be emitted using a different namespace.

3. Choose the metric dimension.
4. Choose the metric that you want from the list, and choose a time period for the graph.

Creating a CloudWatch alarm

You can create a CloudWatch alarm that sends an Amazon Simple Notification Service (Amazon SNS) message when the alarm changes state. An alarm watches a single metric over a time period that you specify. It performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The action is a notification sent to an Amazon SNS topic or an Auto Scaling policy.

Alarms invoke actions for sustained state changes only. CloudWatch alarms don't invoke actions simply because they are in a particular state. The state must have changed and have been maintained for a specified number of time periods.

To create an alarm based on an Amazon Q Business or Q Apps metric, see Create a CloudWatch Alarm Based on a CloudWatch Metric.

To set an alarm (console)

1. Sign in to the AWS Management Console and open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
2. In the navigation pane, choose **Alarms**, and choose **Create Alarm**. This opens the **Create Alarm Wizard**.
3. Choose **Select metric**.
4. In the **All metrics** tab, choose an AWS/QBusiness or AWS/QApps metric for your application, index, and data source. Also set the time as set number of hours, days, weeks, or custom.

5. Choose your statistic. For example, **Average**. Also choose your alarm trigger time period as a set number of minutes, hours, per day, or custom.
6. Choose your threshold to trigger the alarm, whether to use a static value or a band and the condition to meet for the threshold.
7. Choose the alarm state for the trigger, whether the metric must fall outside your set threshold, or another state. Select who/which email to send the alarm notification to.
8. Choose **Next**. Add a name and optional description for your alarm. Choose **Next**.
9. Choose **Create Alarm**.

> **Note**
>
> You can use the `Sum` statistic to aggregate all metrics with the unit `Count`. For more information on CloudWatch statistics and how to use them, see CloudWatch statistics definitions in the *Amazon CloudWatch User Guide*.

Amazon Q Business chat metrics

The following table shows the Chat and conversation management metrics that Amazon Q Business sends to CloudWatch in real time.

Metric name	Unit	Description
`ActionErrorCount`	Count	The number of errors because of actions. Valid dimensions: `ApplicationId` , `PluginId`
`ActionInvocationCount`	Count	The number of actions invoked. Valid dimensions: `ApplicationId` , `PluginId`
`BlockedChatMessages`	Count	The number of chat messages that were blocked by Amazon Q Business due to an admin guardrail configuration. For example, a `BlockedTopic` or `Blocked Phrase`. . Valid dimensions: `ApplicationId`

Metric name	Unit	Description
ChatMessages	Count	The number of chat messages This metric is emitted every time a chat message is processed. Valid dimensions: ApplicationId
ChatMessagesWithAttachment	Count	The number of chat messages with file uploads. Valid dimensions: ApplicationId
ChatMessagesWithNoAnswer	Count	The number of chat messages that resulted in no answer. Valid dimensions: ApplicationId
HallucinatedChatMessages	Count	The number of system-generated chat messages with hallucination. **Note** You can create a hallucination rate metric by combining this metric with the ChatMessages metric. Valid dimensions: ApplicationId
TimeToFirstToken	Milliseconds	The time taken to generate the first token in a chat response. This metric measures the initial response latency for chat interactions. Valid dimensions: API name, ApplicationId
Latency	Milliseconds	The total time taken to complete a chat API request from start to finish. This metric measures the end-to-end response time for chat interactions. Valid dimensions: API name, ApplicationId

Metric name	Unit	Description
`DailyActiveUsers`	Count	The number of active users from the previous day. **Note** This metric is calculated using the *Maximum* statistic. For more information, see CloudWatch statistics definitions. Valid dimensions: `ApplicationId`
`MonthlyActiveUsers`	Count	The total number of unique month-to-date active users. This metric will be calculated from the 00:00 UTC on the first day of the month till 00:00 UTC from the current day. **Note** This metric is calculated using the *Maximum* statistic. For more information, see CloudWatch statistics definitions. Valid dimensions: `ApplicationId`

Metric name	Unit	Description
`WeeklyActiveUsers`	Count	The total number of unique week-to-date active users. This metric will be calculated from 00:00 UTC on Sunday till 00:00 UTC from the current day. **Note** This metric is calculated using the *Maximum* statistic. For more information, see CloudWatch statistics definitions. Valid dimensions: `ApplicationId`
`NewConversations`	Count	The number of new conversations started. Valid dimensions: `ApplicationId`
`ThumbsDownCount`	Count	The feedback count for thumbs down. Valid dimensions: `ApplicationId` , `UsefulnessReason`
`ThumbsUpCount`	Count	The feedback count for thumbs up. Valid dimensions: `ApplicationId` , `UsefulnessReason`

Amazon Q Business API operation metrics

The following table shows the API operation metrics that Amazon Q Business sends to CloudWatch.

Metric name	Unit	Description
`success`	Count	The number of successful API operation calls. This metric is emitted for each successful API operation execution.

Metric name	Unit	Description
		Valid dimensions: `MethodType` , `ApplicationId`
`failure`	Count	The number of failed API operation calls. This metric is emitted for each failed API operation execution. Valid dimensions: `MethodType` , `ApplicationId`
`latency`	Milliseconds	The time taken to complete an API operation call. This metric measures the response time for individual API operations. Valid dimensions: `MethodType` , `ApplicationId`

The `MethodType` dimension can include values such as:

- `ListPlugins`
- (Additional method types may be available depending on API usage)

Amazon Q Business index metrics

The following table shows the Index metrics that Amazon Q Business sends to CloudWatch in real time.

Metric name	Unit	Description
`DocumentCount`	Count	The number of documents. This metric is published every 15 minutes. Valid dimensions: `ApplicationId` , `IndexId`
`Documents Indexed`	Count	The number of documents that were indexed. Valid dimensions: `ApplicationId` , `IndexId`, `DataSourceId`

Metric name	Unit	Description
DocumentsFailedToIndex	Count	The number of documents that failed to index. Valid dimensions: ApplicationId , IndexId, DataSourceId
DocumentsFailedToIndexDueToCDE	Count	The number of documents that failed to index because of custom document enrichment. Valid dimensions: ApplicationId , IndexId, DataSourceId
ExtractedTextSize	MB	Size of the extracted text Valid dimensions: ApplicationId , IndexId
MonthlyDataSyncDuration	Count	Duration of data synchronization operations over a monthly period. Valid dimensions: ApplicationId , IndexId, DataSourceId

Amazon Q Apps metrics

The following table shows the metrics that Amazon Q Apps sends to CloudWatch in real time.

Metric name	Unit	Description	Namespace
ActiveQAppsUsers	Count	The number of Active Q App users. A user is a person who creates, edits or runs the apps. The metric is emitted once every day on UTC midnight. Valid dimensions: ApplicationId	AWS/QApps
ActiveQAppsCreators	Count	The number of Active Q App creators. A creator is a user who creates a Q App in any way, including through magic	AWS/QApps

Metric name	Unit	Description	Namespace
		wand, magic builder, create blank app or duplicate an app. The metric is emitted once every day on UTC midnight. Valid dimensions: `ApplicationId`	
`QAppCreated`	Count	The number of Q Apps created. This metric is emitted every time a Q App is created Valid dimensions: `ApplicationId`	AWS/QApps
`ActiveQApps`	Count	The number of active Q Apps. The active Q App is defined as the app being created, updated or run. Valid dimensions: `ApplicationId`	AWS/QApps
`QAppPublished`	Count	The number of Q Apps that are shared to the library. This metric is emitted every time a Q App is shared to the library. Valid dimensions: `ApplicationId`	AWS/QApps
`QAppExecuted`	Count	The number of Q Apps run. This metric is emitted every time a Q App is run. Valid dimensions: `ApplicationId`	AWS/QApps
`ResourceCount (QAppCountPerApplication)`	Count	The number of total Q Apps in the application environment. This metric is emitted every 5 minutes with Resource dimension populated as `QAppCount PerApplication .` Valid dimensions: `Resouce, ResourceId, Service, Type .`	Usage

Metric name	Unit	Description	Namespace
`ResourceCount (QAppCountPerUser)`	Count	The number of total users set up for the application environment. This metric is emitted every 5 minutes with Resource dimension populated as `QAppCountPerUser`. Valid dimensions: `Resource, ResourceId, Service, Type`.	Usage

Monitoring Amazon Q Business user conversations with Amazon CloudWatch Logs

You can use Amazon CloudWatch Logs to deliver user conversations and response feedback in Amazon Q Business for you to analyze. These logs can be delivered to multiple destinations, such as Amazon CloudWatch, Amazon S3, or Amazon Data Firehose (standard rates apply). We recommend that you set up conversation and feedback logging within five minutes of creating your Amazon Q Business application environment.

The following are examples of tasks you can complete with logs from conversations and response feedback in Amazon Q Business:

- Identify common user queries and pain points by reviewing the chat message content.
- Identify number of system-generated messages that have hallucination.
- Monitor the quality of responses by looking at metrics like `isMessageWithNoAnswer`.
- Understand user sentiment and satisfaction by analyzing the feedback data, including comments and usefulness ratings.
- Generate custom dashboards and reports to track key metrics and trends over time.

Amazon Q Business supports the `EVENT_LOGS` log type that tracks the specifics of conversations in an application. You can use `EVENT_LOGS` to monitor Amazon Q Business in all AWS regions where Amazon Q Business is offered. For more information about the AWS Regions and endpoints currently supported by Amazon Q Business, see Supported Regions.

Logs from conversations might include sensitive or personally identifiable data passed in the chats. You can filter out this information from your logs with the Amazon Q Business console. Or you can mask this data on your logs using CloudWatch Logs masking policies. For more information, see Help protect sensitive log data with masking.

Topics

- Amazon Q Business chat message and feedback log examples
- Permissions for monitoring Amazon Q Business with Amazon CloudWatch Logs
- Enabling Amazon Q Business user conversation logging
- Amazon Q Business conversation log query examples

Amazon Q Business chat message and feedback log examples

The following are examples of Amazon Q Business chat message and feedback logs in CloudWatch Logs.

Chat message

```
{
    "application_id": "<ApplicationId>",
    "event_timestamp": "2024-09-05T19:43:58Z",
    "log_type": "Message",
    "account_id": "<AccountId>",
    "conversation_id": "<conversationId>",
    "system_message_id": "<systemMessageId>",
    "user_message_id": "<userMessageId>",
    "user_message": string,
    "system_message": string,
    "output_metrics_is_message_blocked": boolean,
    "output_metrics_is_message_with_no_answer": boolean,
    "user_email": "<userEmail>"
}
```

Amazon Q Business generated chat message (hallucination detected)

```
{
    "hallucinated_message": "string",
    "application_id": "<ApplicationId>",
    "event_timestamp": "2024-09-05T19:43:58Z",
```

```
    "log_type": "Message",
    "account_id": "<AccountId>",
    "conversation_id": "<conversationId>",
    "system_message_id": "<systemMessageId>",
    "user_message_id": "<userMessageId>",
    "user_message": string,
    "system_message": string,
    "output_metrics_is_message_blocked": boolean,
    "output_metrics_is_message_with_no_answer": boolean,
    "user_email": "<userEmail>"
}
```

Amazon Q Business generated chat message (no hallucination detected)

```
{
    "hallucinated_message": "NO HALLUCINATION DETECTED",
    "application_id": "<ApplicationId>",
    "event_timestamp": "2024-09-05T19:43:58Z",
    "log_type": "Message",
    "account_id": "<AccountId>",
    "conversation_id": "<conversationId>",
    "system_message_id": "<systemMessageId>",
    "user_message_id": "<userMessageId>",
    "user_message": string,
    "system_message": string,
    "output_metrics_is_message_blocked": boolean,
    "output_metrics_is_message_with_no_answer": boolean,
    "user_email": "<userEmail>"
}
```

For system generated messages that have hallucination, you'll see one of the following log descriptions:

- Hallucination mitigation disabled – `hallucinated_message: DISABLED`
- Hallucination mitigation enabled but not triggered – `hallucinated_message: NOT TRIGGERED`
- Hallucination mitigation enabled and triggered, but no hallucinations detected – `hallucinated_message: NO HALLUCINATION DETECTED`
- Hallucination mitigation feature enabled and triggered, and hallucinations detected – `hallucinated_message: string`

Feedback

```
{
    "application_id": "<ApplicationId>",
    "event_timestamp": "2024-09-05T13:13:27Z",
    "log_type": "Feedback",
    "account_id": "<AccountId>",
    "conversation_id": "<conversationId>",
    "system_message_id": "<systemMessageId>",
    "user_message_id": "<userMessageId>",
    "user_message": string,
    "system_message": string,
    "usefulness_reason": "NOT_FACTUALLY_CORRECT" | "HARMFUL_OR_UNSAFE" |
 "INCORRECT_OR_MISSING_SOURCES" | "NOT_HELPFUL" | "FACTUALLY_CORRECT" | "COMPLETE"
 | "RELEVANT_SOURCES" | "HELPFUL" | "NOT_BASED_ON_DOCUMENTS" | "NOT_COMPLETE" |
 "NOT_CONCISE" | "OTHER",
    "usefulness": "NOT_USEFUL" | "USEFUL",
    "comment": string,
    "user_email": "<userEmail>"
}
```

Permissions for monitoring Amazon Q Business with Amazon CloudWatch Logs

To set up Amazon CloudWatch Logs for Amazon Q Business, use the following IAM policy to grant the necessary permissions.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CloudWatchLogsDeliveryPermissions",
            "Effect": "Allow",
            "Action": "logs:CreateDelivery",
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:delivery-source:*",
                "arn:aws:logs:us-east-1:111122223333:delivery:*",
                "arn:aws:logs:us-east-1:111122223333:delivery-destination:*"
            ]
```

```
        },
        {
            "Sid": "QBusinessLogDeliveryPermissions",
            "Effect": "Allow",
            "Action": "qbusiness:AllowVendedLogDeliveryForResource",
            "Resource": [
                "arn:aws:qbusiness:us-
east-1:111122223333:application/application-id"
            ]
        }
    ]
}
```

For example IAM policies with all the required permissions for your specific logging destination, see Enable logging from AWS services in the *Amazon CloudWatch Logs User Guide*.

Enabling Amazon Q Business user conversation logging

You can enable Amazon Q Business user conversation logging within the Amazon Q Business console or using the Amazon CloudWatch Logs API operations.

When you enable logging, you specify a delivery destination for the logs. If you choose Amazon S3, the prefix of logs delivered to the Amazon S3 bucket is `AWSLogs/account-id/AmazonQBusinessLogs/your-region/application-id/year/month/day/hour/`. The files are compressed and named with `Feedback-20240905T19Z_501fec0f.log.gz` or `VendedAnalyticsChat-20240905T19Z_d26ccf9e.log.gz` formats.

> **Important**
>
> Logs might include sensitive or personally identifiable data passed in the chats. You can filter out this information from your logs with the Amazon Q Business console. Or you can mask this data on your logs using CloudWatch Logs masking policies. For more information, see Help protect sensitive log data with masking.

Topics

- Enabling user conversation logging with the Amazon Q Business console
- Enabling user conversation logging with the Amazon CloudWatch Logs API operations

Enabling user conversation logging with the Amazon Q Business console

To enable user conversation logging with the Amazon Q Business console, use the admin controls for your environment to configure log delivery, optionally filter out sensitive information, and then enable logging to start streaming conversation and feedback data.

To enable logging

1. Open the Amazon Q Business console at Amazon Q Business and sign in to your account.
2. In **Applications**, choose the name of your application environment.
3. In the navigation pane, choose **Enhancements** and choose **Admin Controls and Guardrails**.
4. In **Log delivery**, choose **Add** and choose one of the following options.

   - **Amazon CloudWatch Logs** – Enter the **Destination log group** where the logs will be stored. To filter out sensitive or personally identifiable information, choose **Additional settings - optional** and specify the fields to be logged, the output format, and field delimiter.

     For more information about log groups, see Working with log groups and log streams in the *Amazon CloudWatch Logs* user guide.
   - **Amazon S3** – To add delivery to Amazon S3, choose the **Log type** and specify a **Destination S3 bucket**. To filter out sensitive or personally identifiable information, in **Additional settings - optional** specify the fields to be logged, whether to use hive compatible S3 paths, the output format, and the field delimiter.
   - **Amazon Data Firehose** – To add delivery to Amazon Data Firehose, choose the **Log type** and specify a **Destination delivery stream**. To filter out sensitive or personally identifiable information, in **Additional settings - optional** specify the fields to be logged, the output format, and the field delimiter.

     For information about creating a delivery stream, see Create a Firehose delivery stream.

   > **Note**
   >
   > If you want the users' email recorded in your logs, it must be added explicitly as a field in **Additional settings**.

5. Choose **Enable logging** start streaming conversation and feedback data to your logging destination.

Enabling user conversation logging with the Amazon CloudWatch Logs API operations

To enable user conversation logging with the Amazon CloudWatch Logs API operations, you call the PutDeliverySource, PutDeliveryDesintation, and CreateDelivery API operations. For information about quotas for these API operations, see Service quotas.

> **Note**
>
> To enable conversation logging, you need the Amazon Resource Name (ARN) of your environment. To get this ARN, you can use the Amazon Q Business console or the GetApplication API operation. An ARN follows this format: `arn:aws:qbusiness:region:account-id:application/application-id`.

To enable user conversation logging

1. Create a delivery source with the PutDeliverySource Amazon CloudWatch Logs API operation. Give the delivery source a name and for `resourceArn`, specify the ARN of your application. For `logType`, specify `EVENT_LOGS`.

```
{
  "logType": "EVENT_LOGS",
  "name": "my-q-business-application-delivery-source",
  "resourceArn": "arn:aws:qbusiness:your-region:your-account-id:application/
application-id"
}
```

2. Configure the log delivery destination with the PutDeliveryDestination Amazon CloudWatch Logs API operation. You can choose either Amazon CloudWatch Logs, Amazon S3, or Amazon Data Firehose as the destination for storing logs. You must specify the Amazon Resource Name of one of the destination options for where your logs will be stored. The `outputFormat` of the logs can be one of the following: json, plain, w3c, raw, or parquet. The following shows how to specify an Amazon S3 bucket as a log delivery destination with an `outputFormat` of `json`.

```
{
    "deliveryDestinationConfiguration": {
        "destinationResourceArn": "arn:aws:s3:::bucket-name"
```

```
    },
    "name": "s3-delivery-destination",
    "outputFormat": "json",
    "tags": {
        "key": "value"
    }
}
```

3. Enable monitoring with the CreateDelivery Amazon CloudWatch Logs API operation. This API operation links the delivery source to the destination you created in the previous steps.

```
{
  "deliveryDestinationArn": "string",
  "deliverySourceName": "string",
  "tags": {
    "string": "string"
  }
}
```

> **Note**
>
> If you want the users' email recorded in your logs, it must be added explicitly as a field along with the other fields that you want in the `recordFields` parameter as part of calling the `CreateDelivery` operation .

Amazon Q Business conversation log query examples

You can use CloudWatch Logs insights to interact with conversation and feedback logs from Amazon Q Business. The following are examples of common queries.

- Query for all the feedback type logs.

```
filter log_type = "Feedback"
```

- Query for all the chat type logs.

```
filter log_type = "VendedAnalyticsChat"
```

- Query for chat logs related to particular conversation.

```
filter conversation_id = <conversation_id>
```

- Query for chat logs where customer message with certain pattern.

```
filter customer_message like /pattern/
```

- Query for chat logs where system response message with certain pattern.

```
filter system_message like /pattern/
```

- Query for chat logs where system not able to provide answer.

```
filter system_message like /Sorry, I could not find relevant information to complete
 your request./
```

- Query for chat logs where system not able to provide answer.

```
filter output_metrics_is_message_with_no_answer = 1
```

- Query for chat logs where customer message was blocked.

```
filter output_metrics_is_message_blocked = 1
```

- Query for all the feedback logs where system answer was marked useful.

```
filter usefulness = "USEFUL"
```

- Query for all the feedback logs where system answer was marked not useful.

```
filter usefulness = "NOT_USEFUL"
```

- Query for all the feedback logs where system answer was marked not useful with reason “Other”.

```
filter usefulness = "NOT_USEFUL" and usefulness_reason = "OTHER"
```

- Query all feedback logs where system message was hallucinated

```
filter hallucinated_message != "NOT TRIGGERED" and hallucinated_message != NO
 HALLUCINATION DETECTED
```

Viewing Amazon Q Business and Q App metrics in analytics dashboards

The analytics dashboards in Amazon Q Business offer a comprehensive view of key usage metrics and trends about the Amazon Q application environment and Amazon Q Apps. This centralized hub presents the CloudWatch metrics as interactive charts and visualizations for you to review. There are two dashboards:

- Amazon Q Business Analytics dashboard – Use this dashboard to learn how users are interacting with a specific Amazon Q Business application environment. For example, you can identify trends in usage, conversation, feedback, and queries.
- Amazon Q App Analytics dashboard – Use this dashboard to learn how your users are interacting with Q Apps. For example, you can identify the average daily users creating, updating, or running Q Apps over a specific time period.

As an Amazon Q admin, you can view the dashboards with the Amazon Q Business console. You can view the metrics in these dashboards over different pre-selected time intervals. They are available at no additional charge in all Regions where the Amazon Q Business service is offered.

Topics

- Viewing the analytics dashboards
- Amazon Q Business Analytics dashboard metrics
- Amazon Q Apps Analytics dashboard metrics

Viewing the analytics dashboards

To view the Amazon Q Business Analytics dashboard or Amazon Q Apps Analytics dashboard with the Amazon Q Business console, you choose your application environment and navigate to the Analytics dashboard page.

To view the analytics dashboards

1. Sign in to the Amazon Q Business console at https://console.aws.amazon.com/amazonq/business/.
2. In the left navigation pane, choose **Applications**.

3. From the **Applications** section in the center pane, choose the *Name* of application environment that you want to see the Analytics for.
4. In the left navigation pane, choose **Insights**.Choose between **Amazon Q Business** or **Amazon Q Apps** to view the relevant dashboard for your application environment. For information about the metrics that appear, see Amazon Q Business Analytics dashboard metrics orAmazon Q Apps Analytics dashboard metrics.
5. Use the date picker to specify the time interval for the graphs. You can choose from the following preset intervals.

   - Last week – This interval starts from the previous Sunday at 00:00 and goes until the following Sunday at 00:00 in the UTC time zone.
   - This week – This interval starts this Sunday at 00:00 and goes until 00:00 today in the UTC time zone.
   - Last month – This interval begins on the 1st day of the last month at 00:00 and ends on the first day of this month at 00:00 in the UTC time zone.
   - This month – This interval begins on the 1st day of this month at 00:00 and goes until 00:00 today in the UTC time zone.

Amazon Q Business Analytics dashboard metrics

The Amazon Q Business dashboard provides a comprehensive view of key metrics to help admins understand the performance and usage of every Amazon Q application environment from the Amazon Q Business console.

The following analytics are available in the dashboard for the specified time period.

- **Average daily active users**

  This tile gives the average number of unique daily users for the application environment that participated in at least one chat session for the chosen period.

  > **Note**
  >
  > This metric is calculated using the *Maximum* statistic. For more information, see CloudWatch statistics definitions.

- **Total users**

All the users of this application environment.

- **Weekly active users**

  This tile gives the total number of unique users for the application environment who participated in at least one chat session for the week in the chosen period.

- **Monthly active users**

  This tile gives the total number of unique users for the application environment who participated in at least one chat session for the month in the chosen period.

- **Total conversations**

  This tile gives the total number of chat conversations that have occurred in this application environment. Conversations are different from individual chat queries and represent a collection of related queries and responses over a relevant session or subject.

- **Total queries**

  This tile gives the total number of chat message queries received by this application environment.

- **Average queries per user**

  This tile gives the average of daily chat queries for divided by the daily active unique users for that application environment for the chosen period.

- **Average queries per conversation**

  This tile gives the average of total chat queries to an application environment divided by the total individual conversations in the application environment. Conversations refer to new chat threads, which are listed on the left navigation pane of the web experience for the application environment.

- **Total plugins**

  This tile shows the total number of plug-ins currently used by this application environment.

- **Most frequently used plugin**

  This tile shows the plug-in most frequently used by this application environment.

- The **Overview** trend

This line chart displays two trend lines - one showing the daily active users for each day for the application environment, and another showing the total daily individual chat queries received by the application environment.

- The **Customer feedback** trend

  This line chart displays three trend lines for the application environment.

  - The number of thumbs up feedback.
  - The number of thumbs down feedback.
  - The number of chat message responses that did not receive any feedback thumbs up or thumbs down).

- The **Thumbs down reasons** chart

  This pie chart represents the different feedback reasons that users choose when providing a thumbs down feedback, along with the count or percentage of times each reason was selected. You can also filter by feedback reasons to further see the top queries that resulted in the feedback or choose **view details to resolve issues** to see all the queries for further evaluation.

  - The **Thumbs-down feedback queries**

    This page shows the list of queries that resulted in an unsuccessful response for further evaluation. You can choose any query to view details and see **Recommendations** on how to possibly resolve the issue.

    > **Note**
    >
    > - A maximum of *5000* query responses will be loaded initially for evaluation. You can always search for specific queries.
    > - The empty columns in some rows indicate that you need to update the **Vended log deliveries** configuration in **Admin-controls-guardrails page**.

- The **Unsuccessful query responses** chart

  This pie chart represents the breakdown between unsuccessful query responses because the answer was not found or the answer was blocked due to your guardrails settings. You can also filter by response type further to see the top queries that resulted in the response or choose **view details to resolve** issues to see all the queries for further evaluation.

  - The **Unsuccessful response queries**

This page shows the list of queries that resulted in an unsuccessful response for further evaluation. You can choose any query to view details and see **Recommendations** on how to possibly resolve the issue.

> **Note**
>
> - A maximum of *5000* query responses will be loaded initially for evaluation. You can always search for specific queries.
> - The empty columns in some rows indicate that you need to update the **Vended log deliveries** configuration in **Admin-controls-guardrails page**.

- The **Queries** trend

  This chart displays three trend lines.

  - The number of chat queries that included a file upload.
  - The number of instances where the chat queries was blocked by the guardrails set.
  - The number of instances where the application environment was unable to find a relevant answer to the user's query.

- The **Plugins** chart

  This bar chart shows the number of times users have selected each of the available plugins per day. For example, *ServiceNow*, *Salesforce*, *JIRA*, *Zendesk*, *Custom*, etc. when sending a query to the application environment.

- The **Conversations** chart

  This bar chart shows the total number of conversations per day for the specified date range. Conversations are different from individual chat queries, and represent a collection of related queries and responses over a relevant session.

- The **Average queries per conversation** trend

  This bar chart calculates the average number of queries per conversation by dividing the total number of daily queries by the total number of conversations per day for the application environment. Conversations are listed on the left navigation pane of the web experience, and each conversation represents a collection of related chat messages. The chart indicates the average length of conversations, as measured by the total number of chat messages from the first to the last message in a given conversation thread.

Amazon Q Apps Analytics dashboard metrics

The Amazon Q Apps dashboard provides a comprehensive view of key metrics to help admins understand the performance and usage of Q Apps.

If the metrics are not populated in the dashboard, it is likely due to the absence of a Q Apps service role or the role is not configured properly in the Amazon Q Business application environment. Usually a banner will be displayed on the Amazon Q Business console to prompt creating and registering the Q Apps service role.

Depending on how you set up the Amazon Q Business application environment prior to the introduction of analytics dashboard feature, the banner might not always appear. To resolve the issue, go to the **Admin controls and guardrails** page for the Amazon Q Business application environment, choose **Edit Global Control** and re-save the configuration without changes. The metrics should start populating in 10 minutes.

The following analytics are available in the Amazon Q Apps Analytics dashboard for the specified time period.

- **Active users**

  The average unique daily users creating, updating, or running Q Apps.
- **Active creators**

  The average unique daily users creating or updating Q Apps.
- **Total Q Apps**

  The average of the total Q Apps per day.
- **Active Q Apps**

  The average number of daily Q Apps ran or updated.
- **Q App Participants trend**

  A trend of the daily active users and the daily active creators.
- **Q App trend**

  A trend of the total daily Q Apps created and the daily active Q Apps.
- **Total Q Apps Runs trend**

A trend of the total daily Q App runs.

- **Published Q App trend**

  A trend of the total daily published Q Apps.

Maintenance updates for Amazon Q Business

Amazon Q Business periodically performs maintenance updates on its resources. Maintenance most often involves updates to the Amazon Q Business index for security fixes, bug fixes, and other performance enhancements.

Maintenance updates can either be performed automatically by the service on your behalf, or have to manually applied to your Amazon Q Business resources. If a manual maintenance update is required, you must apply it as soon as it is available. If a manual maintenance update is optional, we recommend that you apply it to your Amazon Q Business resources as soon as possible.

Maintenance updates can also have designated maintenance windows. In most cases, the service will inform you of the maintenance update window designated for your Amazon Q Business resources. To minimize the impact of the maintenance on your application, you can reschedule this window by contacting AWS Support.

Amazon Q Business index updates

When your Amazon Q Business index requires an update, you will receive notifications about the update on the Amazon Q Business console or through emails.

Usually, an Amazon Q Business index maintenance update will involve the following:

- Queries will continue to run and work as expected on documents already existing in the index. All other functionality will continue working as expected.
- Data and access control list (ACL) syncs for Amazon Q Business connectors, and documents uploaded directly to an Amazon Q Business application, will be paused. This will be the case no matter how the documents are added to the index—using the console or through the API.
- The status of indexed documents will remain **In progress** for up to 1 day. If you use the API, using the `UpdateIndex` operation will return a 409 status code with the following message: `Index can't be updated at this time due to ongoing maintenance activity. Try again later.`
- All in-progress documents will be synced when the planned maintenance is complete. No data loss will occur.
- For Amazon Q Business applications encrypted with a customer managed KMS key, you'll see CloudTrail events for the following APIs while maintenance is going on:

- CreateGrant
- GenerateDataKey
- Decrypt

All these accesses are authorized use by the Amazon Q Business service and are required for the maintenance activity.

Service quotas for Amazon Q Business

The following are the service endpoints and service quotas for Amazon Q Business To connect programmatically to Amazon Q Business, you use an endpoint. For more information, see AWS service endpoints in the *AWS General Reference*. Service quotas, also referred to as limits, are the maximum number of service resources or operations for your AWS account. For more information, see AWS service quotas in the *AWS General Reference*.

Supported Regions

The following table shows the AWS Regions and endpoints currently supported by Amazon Q Business.

Region name	Region	Endpoint	Protocol
US East (N. Virginia)	us-east-1	qbusiness.us-east-1.api.aws qbusiness-fips.us-east-1.api.aws qbusiness-websocket.us-east-1.api.aws qbusiness-websocket-fips.us-east-1.api.aws	HTTPS
US West (Oregon)	us-west-2	qbusiness.us-west-2.api.aws qbusiness-fips.us-west-2.api.aws qbusiness-websocket.us-west-2.api.aws qbusiness-websocket-fips.us-west-2.api.aws	HTTPS

Region name	Region	Endpoint	Protocol
Europe (Ireland)	eu-west-1	qbusiness-eu-west-1.api.aws qbusiness-websocket.eu-west-1.api.aws	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	qbusiness.ap-southeast-2.api.aws qbusiness-websocket.ap-southeast-2.api.aws	HTTPS

Important

Amazon Q Business Pro tier subscriptions in Europe (Ireland) (eu-west-1) and Asia Pacific (Sydney) (ap-southeast-2) regions are available with a limited set of features.

Note

The Europe (Ireland) and the Asia Pacific (Sydney) regions don't currently support all features available in the US regions, such as Q App, Q Actions, and Audio/Video files. While these features will become available soon, Amazon Q Business customers in this region can do the following:

- Get answers to questions submitted to the enterprise retrieval augmented generation system.
- Generate content through Amazon Q Business assistant
- Access capabilities such as embedded images in files.
- Perform tabular search on small tables.
- Ingest data from scanned PDFs.
- Answer questions from data in scanned PDFs.

- Respond to queries to LLM knowledge.

For a list of AWS regions where Amazon Q Business is available, see Amazon Q Business regions and endpoints in the *Amazon Web Services General Reference*.

Quotas

Your AWS account has default quotas, formerly referred to as limits, for each AWS service. Unless otherwise noted, each quota is Region-specific. You can request increases for some quotas, and other quotas can't be increased. To see whether a quota can be adjusted, refer to the **Adjustable** column in the following table.

To view the quotas for Amazon Q Business, or request a quota increase, open the Service Quotas console. In the navigation pane, choose **AWS services** and select **Amazon Q**.

The following table shows the quotas that are related to Amazon Q Business for your AWS account.

Name	Default	Adjustable	
Maximum number of data accessors per Amazon Q Business application environment	10	No	
Maximum number of applications per account	50	No	
Maximum number of data sources per application	50	No	
Maximum number of plugins per applicati on	25	No	

Name	Default	Adjustable	
Maximum number of actions per plugin	20	No	
Maximum number of transactions per second (TPS) to list actions configured for a specific plugin	10	Yes	
Maximum number of transactions per second (TPS) to list actions and metadata configured for all plugins	5	Yes	
Maximum number of pages per PDF for optical character recognition (OCR) or insight extractio n from embedded visual elements.	3000	No	
Maximum number of pages per Word document for insight extraction from embedded visual elements.	3000	No	

Name	Default	Adjustable	
Maximum number of pages per Powerpoint document for insight extraction from embedded visual elements.	3000	No	
Maximum number of images per PDF, Word or Powerpoint document for insight extraction from embedded visual elements.	500	No	
Maximum number of queries per second (QPS) per index This limit applies to the underlyin g index for your application across all user queries. The SearchRel evantContent, Chat, and ChatSync APIs are throttled differently. For more information, see Chat and conversation management.	1	Yes	

Name	Default	Adjustable
Maximum number of documents that can be uploaded during a conversation or chat session	5	No
Maximum file size per document upload during a conversation or chat session	10 MB	No
Maximum number of total Amazon Q Apps created within an application environment	1000	No
Maximum number of Amazon Q Apps that a single web experience user can create	100	No
Maximum number of cards used per Amazon Q Apps	35	No
Maximum character length for an Amazon Q Apps Creator prompt	10,000	No
Maximum number of file upload cards per Amazon Q Apps	20	No

Name	Default	Adjustable
Maximum file size per file upload card	50 MB	No
Maximum frame rate for video files	60 FPS	No
Maximum file size limit for video files extraction	10 GB	No
Maximum file size limit for audio files extraction	2 GB	No
File size limit in Amazon Q Business File Upload console (all types)	50 MB	No
Maximum duration limit for video files extraction	4 hours	No
Maximum duration limit for audio files extraction	4 hours	No
Maximum number of groups per user supported by Amazon Q Business	1000	No

API reference for Amazon Q Business

For information on Amazon Q Business APIs, see the Amazon Q Business API reference.

For information about the IAM access control permissions you need to use this API, see IAM roles for Amazon Q Business in the *Amazon Q Business User Guide*.

The following resources provide additional information about using the Amazon Q Business API:

- *Setting up for Amazon Q Business*
- *Amazon Q Business CLI Reference*
- *AWS General Reference*

The following pages list Amazon Q Business API actions categorized according to functionality. Links are provided to console procedures and CLI code examples within this User Guide, along with links to corresponding operations in the *Amazon Q Business API Reference*.

Topics

- Creating an Amazon Q Business application using APIs
- Creating an Amazon Q Business index using APIs
- Creating a retriever for an Amazon Q Business application using APIs
- Connecting an Amazon Q Business data source using APIs
- Upload documents directly into a Amazon Q Business application using APIs
- GetDocumentContent Output Schema
- Creating and customizing an Amazon Q Business web experience using APIs
- Chat and conversation management for an Amazon Q Business application using APIs
- Managing users and groups for an Amazon Q Business application using APIs
- Managing subscriptions for an Amazon Q Business application using APIs
- Creating Amazon Q Business plugins using APIs
- Managing admin controls and guardrails using APIs
- User feedback using Amazon Q Business APIs

Creating an Amazon Q Business application using APIs

All Amazon Q Business application environment actions are supported both on the console and using APIs.

API action	API description	Relevant User Guide topic
CreateApplication	Creates an Amazon Q Business application	• Creating an IAM Identity Center-integrated Amazon Q Business application • Creating an IAM federated Amazon Q Business application • Creating an Quick-integrated Amazon Q Business application
DeleteApplication	Deletes an Amazon Q Business application	• Deleting an IAM Identity Center-integrated Amazon Q Business application • Deleting an IAM federated Amazon Q Business application
GetApplication	Gets information about an existing Amazon Q Business application	• Getting properties of an IAM Identity Center-integrated Amazon Q Business application • Getting properties of an IAM federated Amazon Q Business application
ListApplications	Lists existing Amazon Q Business applications	• Listing IAM Identity Center-integrated Amazon Q Business applications • Listing IAM federated Amazon Q Business applications
UpdateApplication	Updates an existing Amazon Q Business application	• Updating an IAM Identity Center-integrated Amazon Q Business application • Updating an IAM federated Amazon Q Business application

Creating an Amazon Q Business index using APIs

All Amazon Q Business index actions are supported both on the console and using APIs.

API action	API description	Relevant User Guide topic
CreateIndex	Creates an Amazon Q Business index	Creating an index
DeleteIndex	Deletes an Amazon Q Business index	Deleting an index
GetIndex	Gets information about an existing Amazon Q Business index	Getting properties of an Amazon Q Business index
ListIndices	Lists existing Amazon Q Business indices	Listing properties of an Amazon Q Business index
UpdateIndex	Updates an existing Amazon Q Business index	Updating an Amazon Q Business index

Creating a retriever for an Amazon Q Business application using APIs

You can't create an Amazon Q Business retriever using the AWS Management Console. If you use the console, Amazon Q Business creates a retriever for you when you create an Amazon Q Business index. If you're using an Amazon Kendra index as retriever, adding an Amazon Kendra index will also add a retriever.

> **Note**
>
> You can only add an Amazon Kendra index as retriever if you have existing Amazon Kendra indexes.

When you use the APIs, you must create a retriever for your Amazon Q Business index separately.

API action	API description	Relevant User Guide topic
CreateRetriever	Creates an Amazon Q Business or Amazon Kendra retriever	• Creating an Amazon Q Business retriever • Creating an Amazon Kendra retriever
DeleteRetriever	Deletes an Amazon Q Business or Amazon Kendra retriever	• Deleting an Amazon Q Business retriever • Deleting an Amazon Kendra retriever
GetRetriever	Gets information about an existing Amazon Q Business or Amazon Kendra retriever	• Getting Amazon Q Business retriever properties • Getting Amazon Kendra retriever properties
ListRetrievers	Lists existing Amazon Q Business or Amazon Kendra retrievers	• Listing retrievers • Getting Amazon Kendra retriever properties
UpdateRetriever	Updates an existing Amazon Q Business or Amazon Kendra retriever	• Updating an Amazon Q Business retriever • Updating an Amazon Kendra retriever

Connecting an Amazon Q Business data source using APIs

Amazon Q Business supports data source connector configuration through both the console and the APIs.

API action	API description	Relevant User Guide topic
CreateDataSource	Creates and connects Amazon Q Business data source	Configuring Amazon Q Business data source connectors
DeleteDataSource	Deletes an Amazon Q Business data source	Deleting a data source connector

API action	API description	Relevant User Guide topic
GetDataSource	Gets information about an existing Amazon Q Business data source	Getting data source connector properties
ListDataSources	Lists existing Amazon Q Business data sources	Listing data source connectors
UpdateDataSource	Updates an existing Amazon Q Business data source	Updating data source connectors
StartDataSourceSyncJobs	Starts an Amazon Q Business data source sync job	Starting data source connector sync jobs
StopDataSourceSyncJobs	Stops an Amazon Q Business data source sync job	Stopping data source connector sync jobs
ListDataSourceSyncJobs	Lists data source sync jobs	Listing data source connector sync jobs

Upload documents directly into a Amazon Q Business application using APIs

Amazon Q Business supports direct document uploads into an Amazon Q Business index using both the console and the APIs.

API action	API description	Relevant User Guide topic
BatchPutDocument	Adds one or more documents to an Amazon Q Business index	Upload documents

API action	API description	Relevant User Guide topic
BatchDeleteDocument	Asynchronously deletes one or more documents added using the BatchPutDocument API from an Amazon Q Business index	Deleting uploaded documents

GetDocumentContent Output Schema

When you use the GetDocumentContent API with `outputFormat` set to `EXTRACTED`, the response returns extracted text content in JSON format. The output schema is presented in JSON format:

```
{
   // always V1 for now
   schemaVersionId: string;

   // always JSON for now
   outputFormat: string;

   // content for plain-text documents
   plainTextDocumentContent: string;

   // content for non-plaintext documents such as PDF, DOCX, PPTX, Audio, Video
   nonPlainTextDocumentContent: List<ExtractedDocumentBodyElement>;
}
```

The schema for non-plaintext documents includes the `ExtractedDocumentBodyElement` which includes:

```
{
   text: string;

  // Allowed values: TEXT, ARTICLE, SECTION, DIV, IMAGE_DESCRIPTION, CODE,
  // TABLE, LIST, URL, HEADER, FOOTER, FORM, MENU, AUDIO, VIDEO
   elementType: string;

   horizontalHeaderIndex: integer;
   verticalHeaderIndex: integer;
   htmlDocumentTitle: string;
```

```
    sectionTitle: string;
    sectionBody: string;
    tableCaption: string;
    tableFooter: string;
    tableRowHeaders: List<List<string>>;
    tableColumnHeaders: List<List<string>>;
    tableRows: List<List<string>>;
    tableRowsCount: integer;
    tableColumnsCount: integer;
    tableId: string;

    tokens: List<struct>;
    {
         value: string;
         startOffsets: integer;
         endOffsets: integer;
    }

    tableType: string;
    tableSummary: string;

    columnInfoList: List<struct>;
    {
         columnName: string;
         columnSummary: string;
         columnType: string;
         columnRepresentativeValues: List<string>
    }

    // Audio/Video specific fields below
    overallSummary: string;

    audioSummaryList: List<struct>;
    {
         summaryText: string;
         startTimeMilliseconds: string;
         endTimeMilliseconds: string;
    }

    videoSummaryList: List<struct>;
    {
         summaryText: string;
         startTimeMilliseconds: string;
         endTimeMilliseconds: string;
```

```
   }

   audioTranscriptList: List<struct>;
   {
        transcriptText: string;
        startTimeMilliseconds: string;
        endTimeMilliseconds: string;
   }

   videoTranscriptList: List<struct>;
   {
        transcriptText: string;
        startTimeMilliseconds: string;
        endTimeMilliseconds: string;
   }
}
```

Example Output

Plaintext Document Example

For plaintext documents, the extracted content is returned in the `plainTextDocumentContent` field:

```
{
  "schemaVersionId": "V1",
  "outputFormat": "JSON",
  "plainTextDocumentContent": "This is the extracted text content from a plain text
 document."
}
```

Creating and customizing an Amazon Q Business web experience using APIs

If you use the console to create your Amazon Q Business application, a web experience is created automatically and connected to your chosen data source.

API action	API description	Relevant User Guide topic
CreateWebExperience	Creates an Amazon Q Business web experience	Creating a web experience
DeleteWebExperience	Deletes an Amazon Q Business web experience	Deleting an Amazon Q Business web experience
GetWebExperience	Gets information about an Amazon Q Business web experience	Getting Amazon Q Business web experience properties
ListWebExperiences	Lists Amazon Q Business web experiences	Listing Amazon Q Business web experiences
UpdateWebExperience	Updates an Amazon Q Business web experience	Updating an Amazon Q Business web experience

Chat and conversation management for an Amazon Q Business application using APIs

Chatting in an Amazon Q Business web experience preview and a deployed Amazon Q Business web experience uses the following API operations.

Important

Amazon Q Business Chat and ChatSync APIs are intended to be activated by end user interactions, not programmatic access. To protect availability, requests exceeding normal user patterns may be throttled. If throttling occurs, first wait and retry later as it is often temporary. However, if throttling persists—or if you believe the throttling is in error—contact AWS Support for troubleshooting assistance.

API action	API description	Relevant User Guide topic
Chat	Starts or continues a streaming Amazon Q Business conversation	• Preview an Amazon Q Business web experience • Customize an Amazon Q Business web experience • Using Amazon Q Business web experiences
ChatSync	Starts or continues a non-streaming Amazon Q Business conversation	• Preview an Amazon Q Business web experience • Customize an Amazon Q Business web experience • Using Amazon Q Business web experiences
DeleteConversation	Deletes an Amazon Q Business web experience conversation	Conversation management
ListConversations	Lists conversations in an Amazon Q Business web experience	Conversation management
ListMessages	Lists messages in an Amazon Q Business web experience	Using Amazon Q Business web experiences

This section outlines how to use Amazon Q Business APIs to make authenticated API calls, and how to configure a streaming chat conversation.

Topics

- Setting up a streaming Amazon Q Business chat using APIs

Setting up a streaming Amazon Q Business chat using APIs

Amazon Q Business provides a streaming Chat API that you can use to deliver chat responses to your end users as a continuing series of partial results. When you use the streaming API, chat responses are transmitted using sequential data packets.

You can configure streaming for your Amazon Q Business application environment in two ways: using WebSockets directly, or using an AWS SDK. The information in this section can be used to for both methods.

If you use WebSockets to configure streaming, a secure WebSockets connection is created to a supported Amazon Q Business endpoint. An example endpoint may look like this: *wss://qbusiness-websocket.us-west-2.api.aws:443/chat*.

> **Important**
>
> We strongly recommend using SDKs to configure streaming instead of using WebSockets directly. SDKs are the simplest and most reliable method for chat streams. To start streaming using an AWS SDK, see Chat in the Amazon Q Business API Reference.

> **Note**
>
> The `qbusiness.<region>.api.aws:8443` has been deprecated in favor of qbusiness-websocket. Use the `qbusiness-websocket.<region>.api.aws:443` endpoint. Although the `qbusiness.<region>.api.aws:8443` endpoint will continue to work it, we recommend using—or migrating to—the new endpoint.

Topics

- Setting up a WebSocket stream
- Handling WebSocket streaming errors
- Event stream encoding
- Data frames

Setting up a WebSocket stream

The key components for a WebSocket protocol for streaming requests with Amazon Q Business are:

- The upgrade request. This contains the query parameters for your request, and a signature that Amazon Q Business uses as a seed signature.
- One or more messages in event stream encoding that contain metadata and chat bytes.

The following section outlines the steps to set up your WebSocket stream.

1. Attach the following policy to the IAM role that makes the request. See Adding IAM policies for more information.

   JSON

```
{
"Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "MyQBusinessWebsocketPolicy",
                "Effect": "Allow",
                "Action": "qbusiness:Chat",
                "Resource": "*"
        }
    ]
}
```

2. To start the session, create a presigned URL in the following format. Line breaks have been added for readability.

```
GET wss://qbusiness-websocket.us-west-2.api.aws:443/chat?
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=access-key%2FYYYYMMDD%2Fus-west-2%2Fqbusiness-
websocket%2Faws4_request
&X-Amz-Date=YYYYMMDDTHHMMSSZ
&X-Amz-Expires=300
&X-Amz-Security-Token=security-token
&X-Amz-Signature=string
&X-Amz-SignedHeaders=host
&chat-
input={"applicationId":"application_id","userId":"test_user@amazon.com","userGroups":null,"
```

> **Note**
>
> The maximum value for `X-Amz-Expires` is 300 seconds (5 minutes).

Additional operations and parameters are listed in the API Reference; parameters common to all AWS API operations are listed in the Common Parameters section.

To construct the URL for your request and create the Signature Version 4 signature, refer to the following steps. Examples are in pseudocode.

a. Create a canonical request. A canonical request is a string that includes information from your request in a standardized format. This ensures that when AWS receives the request, it can calculate the same signature you created for your URL. For more information, see Create a Canonical Request for Signature Version 4.

```
# HTTP verb
method = "GET"
# Service name
service = "qbusiness"
# Region
region = "us-west-2"
# Amazon Q Business streaming endpoint
endpoint = "wss://qbusiness-websocket.us-west-2.api.aws:443"
# Host
host = "qbusiness-websocket.us-west-2.api.aws"
# Date and time of request
amz-date = YYYYMMDDTHHMMSSZ
# Date without time for credential scope
datestamp = YYYYMMDD
```

b. Create a canonical URI, which is the part of the URI between the domain and the query string.

```
canonical_uri = "/chat"
```

c. Create the canonical headers and signed headers. Note the trailing \n in the canonical headers.

- Append the lowercase header name followed by a colon (:).
- Append a comma-separated list of values for that header. Do not sort values in headers that have multiple values.
- Append a new line (\n).

```
canonical_headers = "host:" + host + "\n"
signed_headers = "host"
```

d. Match the algorithm to the hashing algorithm. Use SHA-256.

```
algorithm = "AWS4-HMAC-SHA256"
```

e. Create the credential scope, which scopes the derived key to the date, AWS Region, and service. For example, *20240415*/*us-west-2*/qbusiness/aws4_request.

```
credential_scope = datestamp + "/" + region + "/" + service + "/" +
 "aws4_request"
```

f. Create the canonical query string. Query string values must be URI-encoded and sorted by name.

- Sort the parameter names by character code point in ascending order. Parameters with duplicate names should be sorted by value. For example, a parameter name that begins with the uppercase letter F precedes a parameter name that begins with the lowercase letter b.
- Do not URI-encode any of the unreserved characters that RFC 3986 defines: A-Z, a-z, 0-9, hyphen (-), underscore (_), period (.), and tilde (~).
- Percent-encode all other characters with %XY, where X and Y are hexadecimal characters (0-9 and uppercase A-F). For example, the space character must be encoded as %20 (don't include '+', as some encoding schemes do); extended UTF-8 characters must be in the form %XY%ZA%BC.
- Double-encode any equals (=) characters in parameter values.

```
canonical_querystring  = "X-Amz-Algorithm=" + algorithm
canonical_querystring += "&X-Amz-Credential="+ access key + "%2F" +
 credential_scope
canonical_querystring += "&X-Amz-Date=" + amz_date
canonical_querystring += "&X-Amz-Expires=300"
canonical_querystring += "&X-Amz-Security-Token=" + URI-Encode(token, 'UTF-8',
 safe='')
canonical_querystring += "&X-Amz-SignedHeaders=" + signed_headers
chat_input_string = {
```

```
    "applicationId": "application_id",
    "userId": "testuser@amazon.com",
    "userGroups": None,
    "clientToken": str(uuid.uuid4()),
    "conversationId": None,
    "parentMessageId": None
}
canonical_querystring += "&" + "chat-input" + "=" + URI-
Encode(json.dumps(chat_input_string), 'UTF-8')
```

g. Create a hash of the payload. For a GET request, the payload is an empty string.

```
payload_hash = HashSHA256(("").Encode("utf-8")).Digest()
```

h. Combine the following elements to create the canonical request.

```
canonical_request = method + '\n'
   + canonical_uri + '\n'
   + canonical_querystring + '\n'
   + canonical_headers + '\n'
   + signed_headers + '\n'
   + payload_hash

 string_to_sign =  algorithm + '\n'
   + amz_date + '\n'
   + new_credential_scope + '\n'
   + hashed_canonical_request
```

3. Create the string to sign, which contains meta information about your request. You use the string to sign in the next step when you calculate the request signature. For more information, see Create a String to Sign for Signature Version 4.

```
hashed_canonical_request =
 HashSHA256(canonical_request.Encode("utf-8")).HexDigest()
new_credential_scope = datestamp + '/' + region + '/qbusiness/aws4_request'
string_to_sign=algorithm + "\n"
   + amz_date + "\n"
   + new_credential_scope + "\n"
   + HashSHA256(canonical_request.Encode("utf-8")).HexDigest()
```

4. Calculate the signature. To do this, derive a signing key from your AWS secret access key. For a greater degree of protection, the derived key is specific to the date, service, and AWS Region.

Use this derived key to sign the request. For more information, see Calculate the Signature for AWS Signature Version 4.

Make sure you implement the `GetSignatureKey` function to derive your signing key. If you have not yet derived a signing key, refer to Examples of how to derive a signing key for Signature Version 4.

```
#Create the signing key
signing_key = GetSignatureKey(secret_key, datestamp, region, service)

# Sign the string_to_sign using the signing key
signature = HMAC.new(signing_key, (string_to_sign).Encode("utf-8"),
 Sha256()).HexDigest
```

The function `HMAC(key, data)` represents an HMAC-SHA256 function that returns results in binary format.

5. Add signing information to the request and create the request URL.

   After you calculate the signature, add it to the query string. For more information, see Add the Signature to the Request.

   First, add the authentication information to the query string.

   ```
   canonical_querystring += "&X-Amz-Signature=" + signature
   ```

   Second, create the URL for the request.

   ```
   request_url = endpoint + canonical_uri + "?" + canonical_querystring
   ```

   Use the request URL with your WebSocket library to make the request to Amazon Q Business.

6. The request to Amazon Q Business must include the following headers. Typically these headers are managed by your WebSocket client library.

   ```
   Host: qbusiness-websocketus-west-2.amazonaws.com
   Connection: Upgrade
   Upgrade: websocket
   Origin: URI-of-WebSocket-client
   Sec-WebSocket-Version: 13
   ```

```
Sec-WebSocket-Key: randomly-generated-string <calculated at runtime>
```

7. When Amazon Q Business receives your WebSocket request, it responds with a WebSocket upgrade response. Typically your WebSocket library manages this response and sets up a socket for communications with Amazon Q Business.

   The following is the response from Amazon Q Business. Line breaks have been added for readability.

```
HTTP/1.1 101 WebSocket Protocol Handshake
Connection: upgrade
Upgrade: websocket
websocket-origin: wss://qbusiness-websocket.us-west-2.api.aws:443/chat
websocket-location: qbusiness-websocket.us-west-2.amazonaws.com/api.aws:443/chat?
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=access-key%2FYYYYMMDD%2Fus-west-2%2Fqbusiness%2Faws4_request
&X-Amz-Date=YYYYMMDDTHHMMSSZ
&X-Amz-Expires=300
&X-Amz-Security-Token=security_token
&X-Amz-SignedHeaders=host
&chat-input=%7B%22applicationId%22%3A%20%22aa419bef-ac4e-4c57-9224-
f603e185ac09%22%2C%20%22userId%22%3A%20%testuser%40amazon.com%22%2C%20%22userGroups
%22%3A%20null%2C%20%22clientToken%22%3A%20%2283eb07d9-193c-420c-97c6-
f2f343d13591%22%2C%20%22conversationId%22%3A%20null%2C%20%22parentMessageId%22%3A
%20null%7D
&X-Amz-Signature=Signature Version 4 signature
x-amzn-RequestId: RequestId
sec-websocket-accept: hash-of-the-Sec-WebSocket-Key-header
```

8. Make your WebSocket streaming request.

   After the WebSocket connection is established, the client can start sending a sequence of chat frames, each encoded using event stream encoding.

   Each data frame contains three headers combined with a chunk of raw text bytes; the following table describes these headers.

Header name byte length	Header name (string)	Header value type	Value string byte length	Value string (UTF-8)
13	:content-type	7	24	application/json
11	:event-type	7	10	textEvent
13	:message-type	7	5	event

9. To end the data stream, send an end of input event in an event stream encoded message.

Header name byte length	Header name (string)	Header value type	Value string byte length	Value string (UTF-8)
13	:content-type	7	16	application/json
11	:event-type	7	15	endOfInputEvent
13	:message-type	7	5	event

When you decode the binary response, you end up with a JSON structure containing the chat output.

Handling WebSocket streaming errors

If an exception occurs while processing your request, Amazon Q Business responds with a terminal WebSocket frame containing an event stream encoded response. This response contains the headers described in the following table; the body of the response contains a descriptive error message.

Header name byte length	Header name (string)	Header value type	Value string byte length	Value string (UTF-8)
13	:content-type	7	16	application/json
15	:exception-type	7	varies	varies, see below
13	:message-type	7	9	exception

The `exception-type` header contains one of the following values:

- **`BadRequestException`**: There was a client error when the stream was created, or an error occurred while streaming data. Make sure that your client is ready to accept data and try your request again.
- **`InternalFailureException`**: Amazon Q Business had a problem during the handshake with the client. Try your request again.

Amazon Q Business can also return any of the common service errors. For a list, see Common Errors.

Event stream encoding

Amazon Q Business uses a format called event stream encoding for streaming chat.

Event stream encoding provides bidirectional communication between a client and a server. Chats sent to the Amazon Q Business service are encoded in this format. The response from Amazon Q Business also uses this encoding.

Each message consists of two sections: the prelude and the data. The prelude consists of:

1. The total byte length of the message
2. The combined byte length of all headers

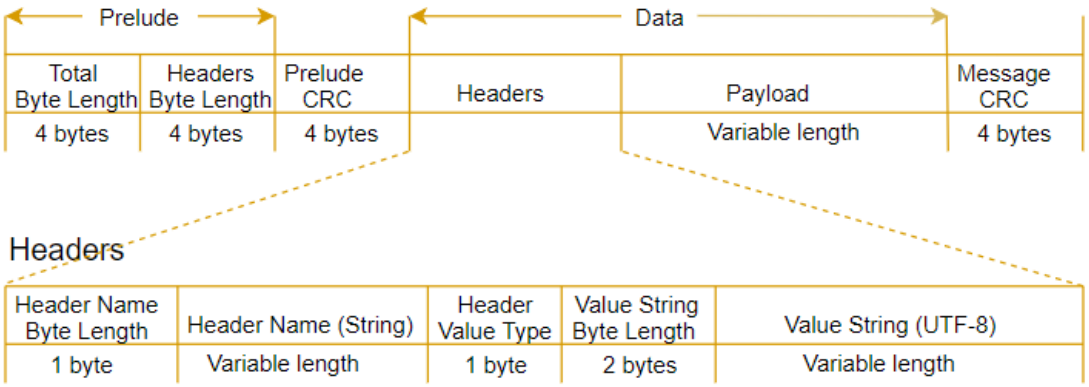
The data section consists of:

1. Headers
2. Payload

Each section ends with a 4-byte big-endian integer cyclic redundancy check (CRC) checksum. The message CRC checksum is for both the prelude section and the data section. Amazon Q Business uses CRC32 (often referred to as GZIP CRC32) to calculate both CRCs. For more information about CRC32, see *GZIP file format specification version 4.3*.

Total message overhead, including the prelude and both checksums, is 16 bytes.

The following diagram shows the components that make up a message and a header. There are multiple headers per message.



Each message contains the following components:

- **Prelude**: Consists of two, 4-byte fields, for a fixed total of 8 bytes.
  - *First 4 bytes*: The big-endian integer byte-length of the entire message, inclusive of this 4-byte length field.
  - *Second 4 bytes*: The big-endian integer byte-length of the 'headers' portion of the message, excluding the 'headers' length field itself.
- **Prelude CRC**: The 4-byte CRC checksum for the prelude portion of the message, excluding the CRC itself. The prelude has a separate CRC from the message CRC. That ensures that Amazon Q Business can detect corrupted byte-length information immediately without causing errors, such as buffer overruns.
- **Headers**: Metadata annotating the message; for example, message type and content type. Messages have multiple headers, which are key:value pairs, where the key is a UTF-8 string. Headers can appear in any order in the 'headers' portion of the message, and each header can appear only once.
- **Payload**: The streaming chat content to be transcribed.
- **Message CRC**: The 4-byte CRC checksum from the start of the message to the start of the checksum. That is, everything in the message except the CRC itself.

The header frame is the authorization frame for the streaming chat. Amazon Q Business uses the authorization header's value as the seed for generating a chain of authorization headers for the data frames in the request.

Each header contains the following components; there are multiple headers per frame.

- **Header name byte-length**: The byte-length of the header name.
- **Header name**: The name of the header that indicates the header type. For valid values, see the following frame descriptions.
- **Header value type**: A number indicating the header value. The following list shows the possible values for the header and what they indicate.
  - `0` – TRUE
  - 1 – FALSE
  - 2 – BYTE
  - 3 – SHORT
  - 4 – INTEGER
  - 5 – LONG
  - 6 – BYTE ARRAY
  - 7 – STRING
  - 8 – TIMESTAMP
  - 9 – UUID
- **Value string byte length**: The byte length of the header value string.
- **Header value**: The value of the header string. Valid values for this field depend on the type of header.

Data frames

Each streaming request contains one or more data frames. There are two steps to creating a data frame:

1. Combine raw `ChatInput` data with metadata to create the payload of your request.
2. Combine the payload with a signature to form the event message that is sent to Amazon Q Business.

Managing users and groups for an Amazon Q Business application using APIs

Amazon Q Business provides APIs to manage users and groups in your Amazon Q Business. You can't configure user management using the console—Amazon Q Business automatically invokes these API operations for you when you configure your data source connector connection. You can use these APIs to implement your own user and group management solution if you create a Amazon Q Business application environment programmatically.

> **Note**
>
> As of Dec 17, 2024, Amazon Q Business will recognize all email addresses as case-insensitive and recognize subaddresses as equivalent to the original email address. For example, JohnDoe@example.com, johndoe@example.com, and johndoe+work@example.com will be considered the same email address. For assistance with applications or to report a concern, contact Support, sign into the AWS Support Center .

API action	API description	Relevant User Guide topic
CreateUser	Creates a universally unique identifier (UUID) mapped to a list of local user ids within an application	User mapping
GetUser	Describes the universally unique identifier (UUID) associated with a local user in a data source	User mapping
UpdateUser	Updates information associated with a user id	User mapping
PutGroup	Creates, or updates, a mapping of users to groups	Group mapping

API action	API description	Relevant User Guide topic
DeleteGroup	Deletes a group so that all users and sub groups that belong to the group can no longer access documents only available to that group	Group mapping
GetGroup	Describes a group by group name	Group mapping
ListGroups	Provides a list of groups that are mapped to users	Group mapping

Managing subscriptions for an Amazon Q Business application using APIs

Amazon Q Business provides APIs to manage subscriptions in your Amazon Q Business application. You can use these APIs to implement your own subscription management solution if you create a Amazon Q Business application environment programmatically.

> **Note**
>
> As of Dec 17, 2024, Amazon Q Business will recognize all email addresses as case-insensitive and recognize subaddresses as equivalent to the original email address. For example, JohnDoe@example.com, johndoe@example.com, and johndoe+work@example.com will be considered the same email address. For assistance with applications or to report a concern, contact Support, sign into the AWS Support Center .

API action	API description	Relevant User Guide topic
CreateSubscription	Subscribes an IAM Identity Center user or a group to a pricing tier for an Amazon Q Business application	• Creating an IAM Identity Center-integrated Amazon Q Business application

API action	API description	Relevant User Guide topic
	Note If you're using IAM federation to manage user and group access to Amazon Q Business, subscript ions are created automatically when a user logs in to their Amazon Q Business application.	• Creating an IAM-federated Amazon Q Business application
CancelSub scription	Unsubscribes a user or a group from their pricing tier in an Amazon Q Business application	• Canceling user subscriptions for IAM Identity Center-integrated applications • Canceling user subscriptions for IAM federated applications
ListSubsc riptions	Lists all subscriptions created in an Amazon Q Business application	• Listing user subscriptions for IAM Identity Center-integrated applications • Listing user subscriptions for IAM federated applications
UpdateSub scription	Updates the pricing tier for an Amazon Q Business subscript ion	• Updating user subscriptions for IAM Identity Center-integrated applications • Updating user subscriptions for IAM federated applications

Creating Amazon Q Business plugins using APIs

Amazon Q Business supports plugin creation through both the console and the APIs.

API action	API description	Relevant User Guide topic
CreatePlugin	Creates an Amazon Q Business plugin	Configuring plugins with Amazon Q Business
DeletePlugin	Deletes an Amazon Q Business plugin	Deleting a plugin
GetPlugin	Gets information about an existing Amazon Q Business plugin	Getting plugin properties
UpdatePlugin	Updates an Amazon Q Business plugin	Updating a plugin
ListPlugins	Lists properties of an Amazon Q Business plugin	Listing plugins
ListPluginActions	Lists configured Amazon Q Business actions for a specific plugin in an Amazon Q Business application. Returns empty responses for custom and legacy built-in plugins.	Listing configured plugin actions
ListPluginTypeActions	Lists configured Amazon Q Business actions for any plugin type. Returns empty responses for custom and legacy built-in plugins.	Listing available plugin actions
ListPluginTypeMetadata	Lists metadata for all Amazon Q Business plugin types. Returns empty responses for custom and legacy built-in plugins.	Listing plugin metadata

Managing admin controls and guardrails using APIs

Amazon Q Business supports admin controls and guardrails configuration through both the console and the APIs.

API action	API description	Relevant User Guide topic
UpdateChatControlsConfiguration	Updates an set of chat controls configured for an existing Amazon Q Business application	• Customizing global controls • Creating topic controls
DeleteChatControlsConfiguration	Deletes chat controls configured for an existing Amazon Q Business application	Deleting topic controls
GetChatControlsConfiguration	Gets information about chat controls configured for an existing Amazon Q Business application.	Getting topic control properties

User feedback using Amazon Q Business APIs

Amazon Q Business captures end user feedback to chat responses to help address any technical issues. You can't configure this feature using the console.

API action	API description	Relevant User Guide topic
PutFeedback	Enables your end user to provide feedback on their Amazon Q Business generated chat responses.	Using web experience

Document history

- **Latest documentation update:** August 14, 2025

The following table describes important changes in each release of Amazon Q Business.

Change	Description	Date
New Agentic RAG feature	Enhance Amazon Q Business standard retrieval augmented generation (RAG) capabilities with agentic workflows. For more information, see Agentic RAG in Amazon Q Business.	August 14, 2025
Added support for Clickable S3 Link Feature	Added support for Clickable S3 Link Feature, allowing users to access source documents from S3 through citation links in chat responses, regardless of whether a source URI is configured.	July 22, 2025
Relevancy tuning replaces metadata boosting on new applications	Admins can now control the search results in Amazon Q Business based on when the document was created or modified or where the document is stored. For more information see Tuning the query results based on document attribute relevancy.	July 1, 2025
New response customization feature	Customize Amazon Q Business chat responses. For more information, see	July 1, 2025

	Customizing responses in Amazon Q Business.	
Amazon Q Business application environments for anonymous access	You can now create Amazon Q Business application environments for anonymous access. For more information, see Creating an Amazon Q Business application environment for anonymous access.	April 29, 2025
New hallucination mitigation feature	Reduce response hallucinations during Amazon Q Business chat. For more information, see Hallucination mitigation in Amazon Q Business.	April 10, 2025
Introducing support to use private Amazon S3 buckets to store web customization artifacts	Save your Amazon Q Business web experience customizations in private S3 buckets. For more information, see Customizing visual themes in your Amazon Q web experience.	March 18, 2025

Introducing the Amazon Q Business integration for Microsoft Word	The Amazon Q Business can enhance your users' Microsoft Word experience by increasing their productivity, bringing Amazon Q Business's AI-powered assistance directly into their daily documentation workflows. For more information, see Integrating Microsoft Word with the Amazon Q Business Add-in.	February 27, 2025
Introducing the Amazon Q Business integration for Microsoft Outlook	The Amazon Q Business can enhance your users' Microsoft Outlook experience by increasing their productivity, bringing Amazon Q Business's AI-powered assistance directly into their daily email workflows. For more information, see Integrating Microsoft Outlook with the Amazon Q Business Add-in.	February 27, 2025
New Amazon Q Business chat orchestration controls	You can now use Amazon Q Business Admin controls and guardrails to configure chat orchestration settings. For more information, see Chat orchestration settings.	February 4, 2025

Amazon Q Business now supports Amazon Kendra GenAI Enterprise Edition indices	You can now use an Amazon Kendra GenAI Enterprise Edition index with Amazon Q Business. For more informati on, see Creating an index for an Amazon Q Business application environment.	December 4, 2024
Q Apps plugins support	Q Apps now supports all Amazon Q Business plugins (built-in and custom, including legacy built-in plugins) with more supported actions. For more information, see Using plugins in Q Apps.	December 3, 2024
New managed policy: QBusinessQuicksightPluginPo licy	The QBusinessQuicksigh tPluginPolicy managed policy provides permissions for an Amazon Q Business application environment to communicate with Amazon Quick.	December 3, 2024
New Quick plugin	You can now use a new fully integrated Quick plugin to get insights from structured data through Amazon Quick. For more information, see Configuring the Quick plugin to get insights from structure d data.	December 3, 2024

New Amazon Q Business plugins	Amazon Q Business now has an updated plugins experienc e with new plugins and more supported actions. For more information, see Plugins.	December 3, 2024
Amazon Quick-integrated Amazon Q Business applicati on environment	You can now create an Amazon Quick-integrated Amazon Q Business applicati on environment. For more information, see Creating an Amazon Quick-integrated Amazon Q Business applicati on environment.	December 3, 2024
Amazon Q Business now supports customizing visual themes	Amazon Q Business offers customization options for your web experience, allowing you to align the interface visual elements with your organization's branding and user needs. For more information, see Customizing visual themes.	December 3, 2024
Amazon Q Business now support data accessors	Amazon Q Business data accessors feature allows you to securely share your enterprise data with verified software providers (ISVs) using the Amazon Q index. For more information, see Data Accessors.	December 3, 2024

Amazon Q Business introduces Amazon Q index for software providers	The Amazon Q index allows independent software vendors (ISVs) to access and integrate a company's data into their application environments, enhancing their customer's end user productivity by providing seamless access to company data sources across the ISV's application environments. . For more information, see Amazon Q index for software providers (ISVs).	December 3, 2024
Introducing the Amazon Q Business Slack integration	The Amazon Q Business can enhance your users' Slack experience by increasing their productivity, bringing Amazon Q Business's AI-powered assistance directly into their daily workflows. . For more information, see Integrating Slack with Amazon Q Business.	December 1, 2024
Introducing the Amazon Q Business Microsoft Teams integration	The Amazon Q Business can enhance your users' Microsoft Teams experience by increasing their productivity, bringing Amazon Q Business's AI-powered assistance directly into their daily workflows. . For more information, see Integrating Microsoft Team with Amazon Q Business.	December 1, 2024

Extracting semantic meaning from embedded visual content	Amazon Q Business can now extract semantic meaning from embedded visual content. For more informati on, see Extracting semantic meaning from embedded visual content.	December 1, 2024
Data collection in Amazon Q Apps	You can now create a data collection app in Q Apps to gather multiple pieces of information from app users. A data collection app can leverage generative AI to analyze the collected data, identify common themes, summarize ideas, and provide actionable insights. For more information, see Data collection in Amazon Q Apps.	November 26, 2024
Introducing the Amazon Q Business browser extensions	The Amazon Q Business browser extension enhances your users' web browsing experience. For more information, see Enhancing web browsing with Amazon Q Business.	November 22, 2024
Smartsheet connector	Amazon Q Business now supports a Smartsheet data source connector. For more information, see Smartsheet.	November 21, 2024

Recent file support	Amazon Q Business now supports recent files. For more information, see IAM role for an Amazon Q Business web experience to update your policy to support this feature.	November 21, 2024
Cross-region inference in Amazon Q Business	Amazon Q Business can now select the optimal region within your geography to process your inference request, maximizing available compute resources and model availability. For more information, see Cross-region inference in Amazon Q Business.	November 19, 2024
Custom labels for Amazon Q Apps	Administrators can now customize the labels available for published Q Apps. For more information, see Custom labels for Amazon Q Apps.	November 7, 2024
Service-linked role support for Amazon Q Apps	Amazon Q Apps now supports a service-linked role for creating application environments with enabled Q Apps. For more information, see Using Service Linked Role for Q Apps .	October 22, 2024

Q App Analytics dashboard	You can now use a new Q App Analytics dashboard to learn how your users are interacti ng with Q Apps. For example, you can identify the average daily users creating, updating, or running Q Apps over a specific time period. For more information, see Viewing Amazon Q Business and Q App metrics in analytics dashboards.	October 22, 2024
New managed policy for Amazon Q Apps: QAppsServ iceRolePolicy	The QAppsServiceRolePo licy managed policy provides permissions to publish metrics.	October 22, 2024
Monitor user conversations with Amazon CloudWatch Logs	You can use Amazon CloudWatch Logs to monitor and analyze user conversat ions and response feedback in Amazon Q Business. For more information, see Monitorin g Amazon Q Business user conversations with Amazon CloudWatch Logs.	October 22, 2024
Monitor Q Apps with Amazon CloudWatch	You can now monitor Q Apps with Amazon CloudWatch metrics. For more informati on, see Monitoring Amazon Q Business and Amazon Q Apps with Amazon CloudWatch .	October 22, 2024

Embed Amazon Q Business into trusted websites	Admins can embed the Amazon Q Business assistant within trusted websites. This allows end users to receive immediate, permissions-aware responses from enterprise data sources, with citations from Amazon Q. For more information, see Amazon Q embedded.	October 15, 2024
Admins can now verify Amazon Q Apps	Admins can review your published apps and update the status to *Verified* if they determine the app meets your organization's criteria. For more information, see Verifying Amazon Q Apps.	September 10, 2024
Identity federation through IAM support	You can now use IAM Federation to manage end user access to Amazon Q Business application environments. For more information, see Creating an Amazon Q Business application environment using IAM Federation.	August 22, 2024

Cross-region IAM Identity Center support	You can now create cross-region IAM Identity Center and Amazon Q Business integrations to manage end user access for your application environment. For more information, see Creating a cross-region IAM Identity Center integration.	July 25, 2024
Introducing new CW metrics for Amazon Q Business	Introducing new chat metrics for Amazon Q. For more information, see Amazon Q Business chat metrics.	July 24, 2024
General availability (GA) of Amazon Q Apps	You can now create lightweight, purpose-built Amazon Q Apps within your broader Amazon Q Business application environment. For more information, see Amazon Q Apps.	July 10, 2024
Amazon Q Business personalized chats	Amazon Q Business now supports personalized chat responses for end users. For more information, see Personalizing chat responses.	July 5, 2024
Amazon Q Business scanned PDF support	Amazon Q Business now supports uploading scanned PDFs into data source connectors and application environments. For more information, see Supported document types.	July 2, 2024

Service-linked role support	Amazon Q Business now supports a service-linked role for creating applicati on environments. For more information, see Using service-linked roles.	April 30, 2024
Preview release of Amazon Q Apps	You can now create lightweig ht, purpose-built Amazon Q Apps within your broader Amazon Q Business applicati on environment. For more information, see Amazon Q Apps.	April 30, 2024
Migrating Amazon Q Business application environments to IAM Identity Center	Amazon Q Business now supports migrating your SAML 2.0 compliant applicati on environment to IAM Identity Center. For more details, see Migrating an Amazon Q Business applicati on environment.	April 30, 2024
Amazon Q Business now supports creating custom plugins	Create custom plugins for your Amazon Q Business application environment. For more details, see Creating custom plugins.	April 30, 2024
Amazon Q Business now supports a streaming chat API	Amazon Q Business now supports a streaming chat API. For more details, see Chat and Setting up a streaming chat.	April 30, 2024

Amazon Q Business general release	Amazon Q Business is now generally available.	April 30, 2024
Amazon Q Business now integrates with IAM Identity Center	You can now use IAM Identity Center to manage user access for your Amazon Q Business application environment. For more details, see How Amazon Q Business works.	April 16, 2024
Amazon Q Business admin controls and guardrails update	The Amazon Q Business now supports new web experienc e chat modes, configurable using admin controls. For more details, see Admin controls and guardrails and Conversation settings.	April 16, 2024
Amazon Q Business (For Business Use) guide name update	The Amazon Q Business (For Business Use) Developer Guide is now called the Amazon Q Business User Guide.	March 29, 2024
Boosting chat results using document attributes	Amazon Q Business now supports boosting content used to generate chat responses using document attributes. For more informati on, see Boosting using document attributes.	February 14, 2024
Preview release	This is the initial preview release of the Amazon Q Business (For Business Use) Developer Guide.	November 28, 2023