API Reference

AWS Certificate Manager

API Version 2015-12-08

AWS Certificate Manager: API Reference

Table of Contents

Welcome **1**
Actions **2**
AddTagsToCertificate 3
Request Syntax 3
Request Parameters 3
Response Elements 4
Errors 4
Examples 6
See Also 7
DeleteCertificate 8
Request Syntax 8
Request Parameters 8
Response Elements 9
Errors 9
Examples 10
See Also 11
DescribeCertificate 12
Request Syntax 12
Request Parameters 12
Response Syntax 13
Response Elements 15
Errors 15
Examples 15
See Also 18
ExportCertificate 19
Request Syntax 19
Request Parameters 19
Response Syntax 20
Response Elements 20
Errors 21
Examples 22
See Also 23
GetAccountConfiguration 25
Response Syntax 25

Response Elements ... 25
Errors ... 25
See Also ... 26
GetCertificate ... 27
Request Syntax ... 27
Request Parameters ... 27
Response Syntax ... 28
Response Elements ... 28
Errors ... 29
Examples ... 29
See Also ... 30
ImportCertificate ... 32
Request Syntax ... 33
Request Parameters ... 33
Response Syntax ... 35
Response Elements ... 35
Errors ... 35
Examples ... 36
See Also ... 37
ListCertificates ... 39
Request Syntax ... 39
Request Parameters ... 39
Response Syntax ... 41
Response Elements ... 42
Errors ... 42
Examples ... 43
See Also ... 44
ListTagsForCertificate ... 45
Request Syntax ... 45
Request Parameters ... 45
Response Syntax ... 46
Response Elements ... 46
Errors ... 46
Examples ... 47
See Also ... 48
PutAccountConfiguration ... 49

Request Syntax ... 49
Request Parameters ... 49
Response Elements ... 50
Errors ... 50
See Also ... 51
RemoveTagsFromCertificate ... 52
Request Syntax ... 52
Request Parameters ... 52
Response Elements ... 53
Errors ... 53
Examples ... 54
See Also ... 55
RenewCertificate ... 57
Request Syntax ... 57
Request Parameters ... 57
Response Elements ... 58
Errors ... 58
Examples ... 58
See Also ... 59
RequestCertificate ... 60
Request Syntax ... 60
Request Parameters ... 61
Response Syntax ... 65
Response Elements ... 66
Errors ... 66
Examples ... 67
See Also ... 69
ResendValidationEmail ... 70
Request Syntax ... 70
Request Parameters ... 70
Response Elements ... 72
Errors ... 72
Examples ... 72
See Also ... 73
RevokeCertificate ... 75
Request Syntax ... 75

Request Parameters ... 75
Response Syntax ... 76
Response Elements ... 76
Errors ... 77
See Also ... 78
SearchCertificates ... 79
Request Syntax ... 79
Request Parameters ... 79
Response Syntax ... 81
Response Elements ... 82
Errors ... 83
Examples ... 83
See Also ... 86
UpdateCertificateOptions ... 88
Request Syntax ... 88
Request Parameters ... 88
Response Elements ... 89
Errors ... 89
Examples ... 90
See Also ... 91
Data Types ... 92
AcmCertificateMetadata ... 94
Contents ... 94
See Also ... 97
AcmCertificateMetadataFilter ... 98
Contents ... 98
See Also ... 100
CertificateDetail ... 101
Contents ... 101
See Also ... 108
CertificateFilter ... 109
Contents ... 109
See Also ... 110
CertificateFilterStatement ... 111
Contents ... 111
See Also ... 112

CertificateMetadata 113
Contents 113
See Also 113
CertificateOptions 114
Contents 114
See Also 115
CertificateSearchResult 116
Contents 116
See Also 117
CertificateSummary 118
Contents 118
See Also 123
CommonNameFilter 124
Contents 124
See Also 124
CustomAttribute 125
Contents 125
See Also 125
DistinguishedName 126
Contents 126
See Also 129
DnsNameFilter 130
Contents 130
See Also 130
DomainValidation 131
Contents 131
See Also 133
DomainValidationOption 134
Contents 134
See Also 135
ExpiryEventsConfiguration 136
Contents 136
See Also 136
ExtendedKeyUsage 137
Contents 137
See Also 138

Filters ... 139
Contents ... 139
See Also ... 140
GeneralName ... 141
Contents ... 141
See Also ... 142
HttpRedirect ... 144
Contents ... 144
See Also ... 144
KeyUsage ... 145
Contents ... 145
See Also ... 145
OtherName ... 146
Contents ... 146
See Also ... 146
RenewalSummary ... 147
Contents ... 147
See Also ... 148
ResourceRecord ... 149
Contents ... 149
See Also ... 149
SubjectAlternativeNameFilter ... 151
Contents ... 151
See Also ... 151
SubjectFilter ... 152
Contents ... 152
See Also ... 152
Tag ... 153
Contents ... 153
See Also ... 153
ThrottlingReason ... 155
Contents ... 155
See Also ... 155
TimestampRange ... 156
Contents ... 156
See Also ... 156

X509AttributeFilter 157
Contents 157
See Also 159
X509Attributes 160
Contents 160
See Also 162
Common Parameters 163
Common Error Types 166

Welcome

Welcome to the AWS Certificate Manager (ACM) API Reference. This guide provides descriptions, syntax, and usage examples for each ACM API operation.

You can use ACM to manage SSL/TLS certificates for your AWS-based websites and applications. For general information about using ACM, see the AWS Certificate Manager User Guide.

Instead of using the ACM API directly, you can use one of the AWS SDKs or command line tools to interact with the ACM API. These tools are available for a variety of programming languages and platforms. For more information, see Tools for Amazon Web Services.

Signing API Requests

You must sign your API requests to ACM using Signature Version 4. When you use the AWS SDKs and command line tools, they sign API requests for you. If you do not use these tools, you must calculate the signature yourself. For more information, see Signature Version 4 Signing Process in the *Amazon Web Services General Reference*.

Actions

The following actions are supported:

- AddTagsToCertificate
- DeleteCertificate
- DescribeCertificate
- ExportCertificate
- GetAccountConfiguration
- GetCertificate
- ImportCertificate
- ListCertificates
- ListTagsForCertificate
- PutAccountConfiguration
- RemoveTagsFromCertificate
- RenewCertificate
- RequestCertificate
- ResendValidationEmail
- RevokeCertificate
- SearchCertificates
- UpdateCertificateOptions

AddTagsToCertificate

Adds one or more tags to an ACM certificate. Tags are labels that you can use to identify and organize your AWS resources. Each tag consists of a `key` and an optional `value`. You specify the certificate on input by its Amazon Resource Name (ARN). You specify the tag by using a key-value pair.

You can apply a tag to just one certificate if you want to identify a specific characteristic of that certificate, or you can apply the same tag to multiple certificates if you want to filter for a common relationship among those certificates. Similarly, you can apply the same tag to multiple resources if you want to specify a relationship among those resources. For example, you can add the same tag to an ACM certificate and an Elastic Load Balancing load balancer to indicate that they are both used by the same website. For more information, see Tagging ACM certificates.

To remove one or more tags, use the RemoveTagsFromCertificate action. To view all of the tags that have been applied to the certificate, use the ListTagsForCertificate action.

Request Syntax

```
{
   "CertificateArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

String that contains the ARN of the ACM certificate to which the tag is to be applied. This must be of the form:

`arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789`

For more information about ARNs, see Amazon Resource Names (ARNs).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Tags

The key-value pair that defines the tag. The tag value is optional.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidParameterException

An input parameter was invalid.

HTTP Status Code: 400

InvalidTagException

One or both of the values that make up the key-value pair is not valid. For example, you cannot specify a tag value that begins with `aws:`.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account or the caller's account cannot be found.

HTTP Status Code: 400

TagPolicyException

A specified tag did not comply with an existing tag policy and was rejected.

HTTP Status Code: 400

ThrottlingException

The request was denied because it exceeded a quota.

throttlingReasons

One or more reasons why the request was throttled.

HTTP Status Code: 400

TooManyTagsException

The request contains too many tags. Try the request again with fewer tags.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

Examples

Add two tags to an ACM certificate

This example illustrates one usage of AddTagsToCertificate.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.AddTagsToCertificate
X-Amz-Date: 20160414T162438Z
User-Agent: aws-cli/1.10.20 Python/2.7.3 Linux/3.13.0-83-generic botocore/1.4.11
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAI44QH8DHBEXAMPLE/20160414/us-east-1/acm/
aws4_request,
SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=370a583d3532f14e0cb34ea51de782e9e5138171184bfede740f5f150251fa2f

{
  "CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012",
  "Tags": [{
    "Key": "website",
    "Value": "example.com"
  },
  {
    "Key": "stack",
    "Value": "production"
  }]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 640bd601-025d-11e6-baa2-cd9f4ef8cda6
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Date: Thu, 14 Apr 2016 16:24:41 GMT
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteCertificate

Deletes a certificate and its associated private key. If this action succeeds, the certificate is not available for use by AWS services integrated with ACM. Deleting a certificate is eventually consistent. The may be a short delay before the certificate no longer appears in the list that can be displayed by calling the ListCertificates action or be retrieved by calling the GetCertificate action.

> **Note**
>
> You cannot delete an ACM certificate that is being used by another AWS service. To delete a certificate that is in use, you must first remove the certificate association using the console or the AWS CLI for the associated service.
> Deleting a certificate issued by a private certificate authority (CA) has no effect on the CA. You will continue to be charged for the CA until it is deleted. For more information, see Deleting Your Private CA in the *AWS Private Certificate Authority User Guide*.

Deleting a certificate issued by a private certificate authority (CA) has no effect on the CA. You will continue to be charged for the CA until it is deleted. For more information, see Deleting your private CA in the *AWS Private Certificate Authority User Guide*.

Request Syntax

```
{
   "CertificateArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

String that contains the ARN of the ACM certificate to be deleted. This must be of the form:

`arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789`

For more information about ARNs, see Amazon Resource Names (ARNs).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

You do not have access required to perform this action.

HTTP Status Code: 400

ConflictException

You are trying to update a resource or configuration that is already being created or updated. Wait for the previous operation to finish and try again.

HTTP Status Code: 400

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

ResourceInUseException

The certificate is in use by another AWS service in the caller's account. Remove the association and try again.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account or the caller's account cannot be found.

HTTP Status Code: 400

ThrottlingException

The request was denied because it exceeded a quota.

throttlingReasons

One or more reasons why the request was throttled.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

Examples

Delete an ACM certificate

This example illustrates one usage of DeleteCertificate.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.DeleteCertificate
X-Amz-Date: 20151222T164207Z
User-Agent: aws-cli/1.9.7 Python/2.7.3 Linux/3.13.0-73-generic botocore/1.3.7
Content-Type: application/x-amz-json-1.1
```

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20151222/us-east-1/acm/
aws4_request,
SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=0b29b04bb5f1ebb5fe9e6b1cbcdeda903b4ed2e06f3abe8a092c0ed1193b4dfc

{
  "CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: ee2db085-a8ca-11e5-9561-b3f6248b5775
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Date: Tue, 22 Dec 2015 16:42:03 GMT
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeCertificate

Returns detailed metadata about the specified ACM certificate.

If you have just created a certificate using the `RequestCertificate` action, there is a delay of several seconds before you can retrieve information about it.

Request Syntax

```
{
   "CertificateArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

The Amazon Resource Name (ARN) of the ACM certificate. The ARN must have the following form:

`arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789`

For more information about ARNs, see Amazon Resource Names (ARNs).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Response Syntax

```
{
   "Certificate": {
      "CertificateArn": "string",
      "CertificateAuthorityArn": "string",
      "CreatedAt": number,
      "DomainName": "string",
      "DomainValidationOptions": [
         {
            "DomainName": "string",
            "HttpRedirect": {
               "RedirectFrom": "string",
               "RedirectTo": "string"
            },
            "ResourceRecord": {
               "Name": "string",
               "Type": "string",
               "Value": "string"
            },
            "ValidationDomain": "string",
            "ValidationEmails": [ "string" ],
            "ValidationMethod": "string",
            "ValidationStatus": "string"
         }
      ],
      "ExtendedKeyUsages": [
         {
            "Name": "string",
            "OID": "string"
         }
      ],
      "FailureReason": "string",
      "ImportedAt": number,
      "InUseBy": [ "string" ],
      "IssuedAt": number,
      "Issuer": "string",
      "KeyAlgorithm": "string",
      "KeyUsages": [
         {
            "Name": "string"
         }
      ],
```

```
      "ManagedBy": "string",
      "NotAfter": number,
      "NotBefore": number,
      "Options": {
         "CertificateTransparencyLoggingPreference": "string",
         "Export": "string"
      },
      "RenewalEligibility": "string",
      "RenewalSummary": {
         "DomainValidationOptions": [
            {
               "DomainName": "string",
               "HttpRedirect": {
                  "RedirectFrom": "string",
                  "RedirectTo": "string"
               },
               "ResourceRecord": {
                  "Name": "string",
                  "Type": "string",
                  "Value": "string"
               },
               "ValidationDomain": "string",
               "ValidationEmails": [ "string" ],
               "ValidationMethod": "string",
               "ValidationStatus": "string"
            }
         ],
         "RenewalStatus": "string",
         "RenewalStatusReason": "string",
         "UpdatedAt": number
      },
      "RevocationReason": "string",
      "RevokedAt": number,
      "Serial": "string",
      "SignatureAlgorithm": "string",
      "Status": "string",
      "Subject": "string",
      "SubjectAlternativeNames": [ "string" ],
      "Type": "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Certificate

Metadata about an ACM certificate.

Type: CertificateDetail object

Errors

For information about the errors that are common to all actions, see Common Error Types.

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account or the caller's account cannot be found.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

Examples

Describe an ACM Certificate

This example illustrates one usage of DescribeCertificate.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.DescribeCertificate
X-Amz-Date: 20151221T203246Z
User-Agent: aws-cli/1.9.7 Python/2.7.3 Linux/3.13.0-71-generic botocore/1.3.7
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAI44QH8DHBEXAMPLE/20151221/us-east-1/acm/
aws4_request,
SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=76913a7d6013d34afbdc1bbd6c3e77d5edd3fa2d9883a94d946c6eeea5908d9e

{
  "CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: fd1e5a07-a821-11e5-845d-95c070464235
Content-Type: application/x-amz-json-1.1
Content-Length: 1035
Date: Mon, 21 Dec 2015 20:32:43 GMT

{
  "Certificate": {
    "CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012",
    "CreatedAt": 1450212224.0,
    "DomainName": "example.com",
    "DomainValidationOptions": [
      {
        "DomainName": "example.com",
        "ValidationDomain": "example.com",
        "ValidationEmails": [
          "hostmaster@example.com",
          "admin@example.com",
          "postmaster@example.com",
          "webmaster@example.com",
          "administrator@example.com"
        ]
```

```
      },
      {
        "DomainName": "www.example.com",
        "ValidationDomain": "www.example.com",
        "ValidationEmails": [
          "hostmaster@example.com",
          "admin@example.com",
          "postmaster@example.com",
          "webmaster@example.com",
          "administrator@example.com"
        ]
      }
    ],
    "InUseBy": [
      "arn:aws:cloudfront::111122223333:distribution/E12KXPQHVLSYVC"
    ],
    "IssuedAt": 1450212292.0,
    "Issuer": "Amazon",
    "KeyAlgorithm": "RSA-2048",
    "NotAfter": 1484481600.0,
    "NotBefore": 1450137600.0,
    "Renewal Elegibility": "ELIGIBLE",
    "RenewalSummary": {
         "DomainValidationOptions": [
            {
               "DomainName": "www.example.com",
               "ResourceRecord": {
                  "Name": "example",
                  "Type": "CNAME",
                  "Value": "example"
               },
               "ValidationDomain": "www.amazon.com",
               "ValidationEmails": [ "example@amazon.com" ],
               "ValidationMethod": "DNS",
               "ValidationStatus": "SUCCESS"
            }
         ],
         "RenewalStatus": "SUCCESS",
         "UpdatedAt": 1450212224.0
      },
    "Serial": "07:71:71:f4:6b:e7:bf:63:87:e6:ad:3c:b2:0f:d0:5b",
    "SignatureAlgorithm": "SHA256WITHRSA",
    "Status": "ISSUED",
    "Subject": "CN=example.com",
```

```
    "SubjectAlternativeNames": [
      "example.com",
      "www.example.com"
    ]
  }
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ExportCertificate

Exports a private certificate issued by a private certificate authority (CA) or a public certificate for use anywhere. The exported file contains the certificate, the certificate chain, and the encrypted private key associated with the public key that is embedded in the certificate. For security, you must assign a passphrase for the private key when exporting it.

For information about exporting and formatting a certificate using the ACM console or AWS CLI, see Export a private certificate and Export a public certificate.

> **Note**
>
> ACM public certificates created prior to June 17, 2025 cannot be exported.

Request Syntax

```
{
   "CertificateArn": "string",
   "Passphrase": blob
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

An Amazon Resource Name (ARN) of the issued certificate. This must be of the form:

`arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012`

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Passphrase

Passphrase to associate with the encrypted exported private key.

> **Note**
>
> When creating your passphrase, you can use any ASCII character except #, $, or %.

If you want to later decrypt the private key, you must have the passphrase. You can use the following OpenSSL command to decrypt a private key. After entering the command, you are prompted for the passphrase.

```
openssl rsa -in encrypted_key.pem -out decrypted_key.pem
```

Type: Base64-encoded binary data object

Length Constraints: Minimum length of 4. Maximum length of 128.

Required: Yes

Response Syntax

```
{
   "Certificate": "string",
   "CertificateChain": "string",
   "PrivateKey": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Certificate

The base64 PEM-encoded certificate.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 32768.

Pattern: `-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64}\u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)?`

CertificateChain

The base64 PEM-encoded certificate chain. This does not include the certificate that you are exporting.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2097152.

Pattern: `(-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64}\u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}\u000D?\u000A)*-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64}\u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)?`

PrivateKey

The encrypted private key associated with the public key in the certificate. The key is output in PKCS #8 format and is base64 PEM-encoded.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 524288.

Pattern: `-{5}BEGIN PRIVATE KEY-{5}\u000D?\u000A([A-Za-z0-9/+]{64}\u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END PRIVATE KEY-{5}(\u000D?\u000A)?`

Errors

For information about the errors that are common to all actions, see Common Error Types.

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

RequestInProgressException

The certificate request is in process and the certificate in your account has not yet been issued.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account or the caller's account cannot be found.

HTTP Status Code: 400

ThrottlingException

The request was denied because it exceeded a quota.

throttlingReasons

One or more reasons why the request was throttled.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of ExportCertificate.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
```

```
Accept-Encoding: identity
Content-Length: 135
X-Amz-Target: CertificateManager.ExportCertificate
X-Amz-Date: 20180331T175638Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=key_ID/20180331/us-east-1/acm/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=7b3f783da1b701aea1b6b49dea7d5194d7e2b253f152cfb939459ba3b0ba2c1d

{
  "CertificateArn": "arn:aws:acm:us-
east-1:account:certificate/12345678-1234-1234-1234-1234556789012",
  "Passphrase": "cGFzc3dvcmQ="
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: dd520651-350c-11e8-a99a-c76ec78904bf
Content-Type: application/x-amz-json-1.1
Content-Length: 5860
Date: Sat, 31 Mar 2018 17:56:41 GMT
Connection: Keep-alive

{
  "Certificate":
    "-----BEGIN CERTIFICATE-----Base64-encodedEND CERTIFICATE-----",
  "CertificateChain":
    "-----BEGIN CERTIFICATE-----Base64-encodedEND CERTIFICATE-----
     -----BEGIN CERTIFICATE-----Base64-encodedEND CERTIFICATE-----",
  "PrivateKey":
    "-----BEGIN ENCRYPTED PRIVATE KEYBase64-encoded-----END ENCRYPTED PRIVATE KEY-----"
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetAccountConfiguration

Returns the account configuration options associated with an AWS account.

Response Syntax

```
{
   "ExpiryEvents": {
      "DaysBeforeExpiry": number
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

ExpiryEvents

Expiration events configuration options associated with the AWS account.

Type: ExpiryEventsConfiguration object

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

You do not have access required to perform this action.

HTTP Status Code: 400

ThrottlingException

The request was denied because it exceeded a quota.

throttlingReasons

One or more reasons why the request was throttled.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetCertificate

Retrieves a certificate and its certificate chain. The certificate may be either a public or private certificate issued using the ACM `RequestCertificate` action, or a certificate imported into ACM using the `ImportCertificate` action. The chain consists of the certificate of the issuing CA and the intermediate certificates of any other subordinate CAs. All of the certificates are base64 encoded. You can use OpenSSL to decode the certificates and inspect individual fields.

Request Syntax

```
{
   "CertificateArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

String that contains a certificate ARN in the following format:

`arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789`

For more information about ARNs, see Amazon Resource Names (ARNs).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Response Syntax

```
{
   "Certificate": "string",
   "CertificateChain": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Certificate

The ACM-issued certificate corresponding to the ARN specified as input.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 32768.

Pattern: `-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64}\u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)?`

CertificateChain

Certificates forming the requested certificate's chain of trust. The chain consists of the certificate of the issuing CA and the intermediate certificates of any other subordinate CAs.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2097152.

Pattern: `(-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64}\u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}\u000D?\u000A)*-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64}\u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)?`

Errors

For information about the errors that are common to all actions, see Common Error Types.

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

RequestInProgressException

The certificate request is in process and the certificate in your account has not yet been issued.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account or the caller's account cannot be found.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

Examples

Get an ACM Certificate

This example illustrates one usage of GetCertificate.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.GetCertificate
X-Amz-Date: 20151221T210018Z
User-Agent: aws-cli/1.9.7 Python/2.7.3 Linux/3.13.0-71-generic botocore/1.3.7
Content-Type: application/x-amz-json-1.1
```

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAI44QH8DHBEXAMPLE/20151221/us-east-1/acm/
aws4_request,
SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=b51b4c2d5518473a8552fdab8e313c76254e9ca64e4d8ab69c2ebef83dbd459b

{
  "CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: d5300b5a-a825-11e5-9141-fbb8a078e3eb
Content-Type: application/x-amz-json-1.1
Content-Length: 6506
Date: Mon, 21 Dec 2015 21:00:15 GMT

{
  "Certificate":
    "-----BEGIN CERTIFICATE-----Base64-encoded-----END CERTIFICATE-----",
  "CertificateChain":
    "-----BEGIN CERTIFICATE-----Base64-encoded-----END CERTIFICATE-----"
    "-----BEGIN CERTIFICATE-----Base64-encoded-----END CERTIFICATE-----"
    "-----BEGIN CERTIFICATE-----Base64-encoded-----END CERTIFICATE-----"
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ImportCertificate

Imports a certificate into AWS Certificate Manager (ACM) to use with services that are integrated with ACM. Note that integrated services allow only certificate types and keys they support to be associated with their resources. Further, their support differs depending on whether the certificate is imported into IAM or into ACM. For more information, see the documentation for each service. For more information about importing certificates into ACM, see Importing Certificates in the *AWS Certificate Manager User Guide*.

> **Note**
>
> ACM does not provide managed renewal for certificates that you import.

Note the following guidelines when importing third party certificates:

- You must enter the private key that matches the certificate you are importing.
- The private key must be unencrypted. You cannot import a private key that is protected by a password or a passphrase.
- The private key must be no larger than 5 KB (5,120 bytes).
- The certificate, private key, and certificate chain must be PEM-encoded.
- The current time must be between the `Not Before` and `Not After` certificate fields.
- The `Issuer` field must not be empty.
- The OCSP authority URL, if present, must not exceed 1000 characters.
- To import a new certificate, omit the `CertificateArn` argument. Include this argument only when you want to replace a previously imported certificate.
- When you import a certificate by using the CLI, you must specify the certificate, the certificate chain, and the private key by their file names preceded by `fileb://`. For example, you can specify a certificate saved in the `C:\temp` folder as `fileb://C:\temp\certificate_to_import.pem`. If you are making an HTTP or HTTPS Query request, include these arguments as BLOBs.
- When you import a certificate by using an SDK, you must specify the certificate, the certificate chain, and the private key files in the manner required by the programming language you're using.

- The cryptographic algorithm of an imported certificate must match the algorithm of the signing CA. For example, if the signing CA key type is RSA, then the certificate key type must also be RSA.

This operation returns the Amazon Resource Name (ARN) of the imported certificate.

Request Syntax

```
{
   "Certificate": blob,
   "CertificateArn": "string",
   "CertificateChain": blob,
   "PrivateKey": blob,
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

Certificate

The certificate to import.

Type: Base64-encoded binary data object

Length Constraints: Minimum length of 1. Maximum length of 32768.

Required: Yes

PrivateKey

The private key that matches the public key in the certificate.

Type: Base64-encoded binary data object

Length Constraints: Minimum length of 1. Maximum length of 5120.

Required: Yes

CertificateArn

The Amazon Resource Name (ARN) of an imported certificate to replace. To import a new certificate, omit this field.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: No

CertificateChain

The PEM encoded certificate chain.

Type: Base64-encoded binary data object

Length Constraints: Minimum length of 1. Maximum length of 2097152.

Required: No

Tags

One or more resource tags to associate with the imported certificate.

Note: You cannot apply tags when reimporting a certificate.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Required: No

Response Syntax

```
{
   "CertificateArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CertificateArn

The Amazon Resource Name (ARN) of the imported certificate.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Errors

For information about the errors that are common to all actions, see Common Error Types.

ConflictException

You are trying to update a resource or configuration that is already being created or updated. Wait for the previous operation to finish and try again.

HTTP Status Code: 400

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidParameterException

An input parameter was invalid.

HTTP Status Code: 400

InvalidTagException

One or both of the values that make up the key-value pair is not valid. For example, you cannot specify a tag value that begins with `aws:`.

HTTP Status Code: 400

LimitExceededException

An ACM quota has been exceeded.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account or the caller's account cannot be found.

HTTP Status Code: 400

TagPolicyException

A specified tag did not comply with an existing tag policy and was rejected.

HTTP Status Code: 400

TooManyTagsException

The request contains too many tags. Try the request again with fewer tags.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

Examples

Import a certificate

This example illustrates one usage of ImportCertificate.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.ImportCertificate
X-Amz-Date: 20161011T184744Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=key_ID/20161011/us-east-1/acm/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=60f965247476c4672c498c24ba255e52a62a7e4bd8678d8ee788af5ffe42f377

{
    "CertificateChain": "Base64-encoded blob",
    "PrivateKey": "Base64-encoded blob",
    "Certificate": "Base64-encoded blob"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 32f9ab0a-8fe3-11e6-8d69-c91606b24a3f
Content-Type: application/x-amz-json-1.1
Content-Length: 104
Date: Tue, 11 Oct 2016 18:47:46 GMT

{"CertificateArn":"arn:aws:acm:us-east-1:111122223333:certificate/91228a40-
ad89-4ce0-9f6c-07009fc8fdfb"}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListCertificates

Retrieves a list of certificate ARNs and domain names. You can request that only certificates that match a specific status be listed. You can also filter by specific attributes of the certificate. Default filtering returns only RSA_2048 certificates. For more information, see Filters.

Request Syntax

```
{
   "CertificateStatuses": [ "string" ],
   "Includes": {
      "exportOption": "string",
      "extendedKeyUsage": [ "string" ],
      "keyTypes": [ "string" ],
      "keyUsage": [ "string" ],
      "managedBy": "string"
   },
   "MaxItems": number,
   "NextToken": "string",
   "SortBy": "string",
   "SortOrder": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

CertificateStatuses

Filter the certificate list by status value.

Type: Array of strings

Valid Values: PENDING_VALIDATION | ISSUED | INACTIVE | EXPIRED | VALIDATION_TIMED_OUT | REVOKED | FAILED

Required: No

Includes

Filter the certificate list. For more information, see the Filters structure.

Type: Filters object

Required: No

MaxItems

Use this parameter when paginating results to specify the maximum number of items to return in the response. If additional items exist beyond the number you specify, the `NextToken` element is sent in the response. Use this `NextToken` value in a subsequent request to retrieve additional items.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

NextToken

Use this parameter only when paginating results and only in a subsequent request after you receive a response with truncated results. Set it to the value of `NextToken` from the response you just received.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10000.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Required: No

SortBy

Specifies the field to sort results by. If you specify `SortBy`, you must also specify `SortOrder`.

Type: String

Valid Values: `CREATED_AT`

Required: No

SortOrder

Specifies the order of sorted results. If you specify `SortOrder`, you must also specify `SortBy`.

Type: String

Valid Values: `ASCENDING | DESCENDING`

Required: No

Response Syntax

```
{
   "CertificateSummaryList": [
      {
         "CertificateArn": "string",
         "CreatedAt": number,
         "DomainName": "string",
         "Exported": boolean,
         "ExportOption": "string",
         "ExtendedKeyUsages": [ "string" ],
         "HasAdditionalSubjectAlternativeNames": boolean,
         "ImportedAt": number,
         "InUse": boolean,
         "IssuedAt": number,
         "KeyAlgorithm": "string",
         "KeyUsages": [ "string" ],
         "ManagedBy": "string",
         "NotAfter": number,
         "NotBefore": number,
         "RenewalEligibility": "string",
         "RevokedAt": number,
         "Status": "string",
         "SubjectAlternativeNameSummaries": [ "string" ],
         "Type": "string"
      }
   ],
   "NextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CertificateSummaryList

A list of ACM certificates.

Type: Array of CertificateSummary objects

NextToken

When the list is truncated, this value is present and contains the value to use for the `NextToken` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10000.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Errors

For information about the errors that are common to all actions, see Common Error Types.

InvalidArgsException

One or more of request parameters specified is not valid.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

Examples

List Certificates

The following example lists certificates that you can use to create digital signatures and to sign code.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
Accept-Encoding: identity
Content-Length: 129
X-Amz-Target: CertificateManager.ListCertificates
X-Amz-Date: 20171118T204928Z
User-Agent: aws-cli/1.11.132 Python/2.7.9 Windows/8 botocore/1.5.95
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=key_ID/20171118/us-east-1/acm/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=49a54...

{
 "MaxItems": 10,
 "Includes": {
  "keyUsage": ["DIGITAL_SIGNATURE"],
  "keyTypes": ["RSA_2048"],
  "extendedKeyUsage": ["CODE_SIGNING"]
 }
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: fa8ffa7f-cca1-11e7-80db-736b2201613a
Content-Type: application/x-amz-json-1.1
Content-Length: 164
Date: Sat, 18 Nov 2017 20:49:32 GMT
Connection: Keep-alive
```

```
{"CertificateSummaryList": [
  {
    "CertificateArn":
 "arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012",
    "DomainName": "www.example.com"
  },
  {
    "CertificateArn":
 "arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012",
    "DomainName": "www.corp.net"
  }
]
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTagsForCertificate

Lists the tags that have been applied to the ACM certificate. Use the certificate's Amazon Resource Name (ARN) to specify the certificate. To add a tag to an ACM certificate, use the AddTagsToCertificate action. To delete a tag, use the RemoveTagsFromCertificate action.

Request Syntax

```
{
   "CertificateArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

String that contains the ARN of the ACM certificate for which you want to list the tags. This must have the following form:

`arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789`

For more information about ARNs, see Amazon Resource Names (ARNs).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Response Syntax

```
{
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Tags

The key-value pairs that define the applied tags.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Error Types.

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account or the caller's account cannot be found.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

Examples

List tags for an ACM Certificate

This example illustrates one usage of ListTagsForCertificate.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.ListTagsForCertificate
X-Amz-Date: 20160414T162913Z
User-Agent: aws-cli/1.10.20 Python/2.7.3 Linux/3.13.0-83-generic botocore/1.4.11
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=key_ID/20160414/us-east-1/acm/aws4_request,
SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=c1b80f2b1b6c73c39e1a9594e621648e673b1419101809239b9a5dd8c397953a

{"CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012"}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 07c10419-025e-11e6-baa2-cd9f4ef8cda6
Content-Type: application/x-amz-json-1.1
Content-Length: 87
Date: Thu, 14 Apr 2016 16:29:16 GMT

{
  "Tags": [{
    "Key": "stack",
    "Value": "production"
  },
  {
    "Key": "website",
```

```
    "Value": "example.com"
  }]
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutAccountConfiguration

Adds or modifies account-level configurations in ACM.

The supported configuration option is `DaysBeforeExpiry`. This option specifies the number of days prior to certificate expiration when ACM starts generating `EventBridge` events. ACM sends one event per day per certificate until the certificate expires. By default, accounts receive events starting 45 days before certificate expiration.

Request Syntax

```
{
   "ExpiryEvents": {
      "DaysBeforeExpiry": number
   },
   "IdempotencyToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

IdempotencyToken

Customer-chosen string used to distinguish between calls to `PutAccountConfiguration`. Idempotency tokens time out after one hour. If you call `PutAccountConfiguration` multiple times with the same unexpired idempotency token, ACM treats it as the same request and returns the original result. If you change the idempotency token for each call, ACM treats each call as a new request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 32.

Pattern: \w+

Required: Yes

ExpiryEvents

Specifies expiration events associated with an account.

Type: ExpiryEventsConfiguration object

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

You do not have access required to perform this action.

HTTP Status Code: 400

ConflictException

You are trying to update a resource or configuration that is already being created or updated. Wait for the previous operation to finish and try again.

HTTP Status Code: 400

ThrottlingException

The request was denied because it exceeded a quota.

throttlingReasons

One or more reasons why the request was throttled.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

RemoveTagsFromCertificate

Remove one or more tags from an ACM certificate. A tag consists of a key-value pair. If you do not specify the value portion of the tag when calling this function, the tag will be removed regardless of value. If you specify a value, the tag is removed only if it is associated with the specified value.

To add tags to a certificate, use the AddTagsToCertificate action. To view all of the tags that have been applied to a specific ACM certificate, use the ListTagsForCertificate action.

Request Syntax

```
{
   "CertificateArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

String that contains the ARN of the ACM Certificate with one or more tags that you want to remove. This must be of the form:

`arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789`

For more information about ARNs, see Amazon Resource Names (ARNs).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Tags

The key-value pair that defines the tag to remove.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidParameterException

An input parameter was invalid.

HTTP Status Code: 400

InvalidTagException

One or both of the values that make up the key-value pair is not valid. For example, you cannot specify a tag value that begins with `aws:`.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account or the caller's account cannot be found.

HTTP Status Code: 400

TagPolicyException

A specified tag did not comply with an existing tag policy and was rejected.

HTTP Status Code: 400

ThrottlingException

The request was denied because it exceeded a quota.

throttlingReasons

One or more reasons why the request was throttled.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

Examples

Remove two tags from an ACM certificate

This example illustrates one usage of RemoveTagsFromCertificate.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.RemoveTagsFromCertificate
X-Amz-Date: 20160414T163042Z
User-Agent: aws-cli/1.10.20 Python/2.7.3 Linux/3.13.0-83-generic botocore/1.4.11
Content-Type: application/x-amz-json-1.1
```

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAI44QH8DHBEXAMPLE/20160414/us-east-1/acm/
aws4_request,
SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=379429306c5e89b9b4be5b35e29c26cc1da38215d8055a5ed0bdda57bcc881cc

{
  "CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012",
  "Tags": [{
    "Key": "website",
    "Value": "example.com"
  },
  {
    "Key": "stack",
    "Value": "production"
  }]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 3c8d676d-025e-11e6-8823-93164b47113c
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Date: Thu, 14 Apr 2016 16:30:44 GMT
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

RenewCertificate

Renews an eligible ACM certificate. In order to renew your AWS Private CA certificates with ACM, you must first grant the ACM service principal permission to do so. For more information, see Testing Managed Renewal in the ACM User Guide.

Request Syntax

```
{
   "CertificateArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

String that contains the ARN of the ACM certificate to be renewed. This must be of the form:

`arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789`

For more information about ARNs, see Amazon Resource Names (ARNs).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

RequestInProgressException

The certificate request is in process and the certificate in your account has not yet been issued.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account or the caller's account cannot be found.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

Examples

Renew an ACM Certificate

This example illustrates one usage of RenewCertificate.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
```

```
X-Amz-Target: CertificateManager.RenewCertificate
X-Amz-Date: 20190124T171503Z
User-Agent: aws-cli/1.10.20 Python/2.7.3 Linux/3.13.0-83-generic botocore/1.4.11
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAI44QH8DHBEXAMPLE/20160414/us-east-1/acm/
aws4_request,
SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=379429306c5e89b9b4be5b35e29c26cc1da38215d8055a5ed0bdda57bcc881cc

{
  "CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 3c8d676d-025e-11e6-8823-93164b47113c
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Date: Thu, 24 Jan 2019 17:15:05 GMT
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

RequestCertificate

Requests an ACM certificate for use with other AWS services. To request an ACM certificate, you must specify a fully qualified domain name (FQDN) in the `DomainName` parameter. You can also specify additional FQDNs in the `SubjectAlternativeNames` parameter.

If you are requesting a private certificate, domain validation is not required. If you are requesting a public certificate, each domain name that you specify must be validated to verify that you own or control the domain. You can use DNS validation or email validation. We recommend that you use DNS validation.

> **Note**
>
> ACM behavior differs from the RFC 6125 specification of the certificate validation process. ACM first checks for a Subject Alternative Name, and, if it finds one, ignores the common name (CN).

After successful completion of the `RequestCertificate` action, there is a delay of several seconds before you can retrieve information about the new certificate.

Request Syntax

```
{
   "CertificateAuthorityArn": "string",
   "DomainName": "string",
   "DomainValidationOptions": [
      {
         "DomainName": "string",
         "ValidationDomain": "string"
      }
   ],
   "IdempotencyToken": "string",
   "KeyAlgorithm": "string",
   "ManagedBy": "string",
   "Options": {
      "CertificateTransparencyLoggingPreference": "string",
      "Export": "string"
   },
   "SubjectAlternativeNames": [ "string" ],
```

```
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "ValidationMethod": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

DomainName

Fully qualified domain name (FQDN), such as www.example.com, that you want to secure with an ACM certificate. Use an asterisk (*) to create a wildcard certificate that protects several sites in the same domain. For example, *.example.com protects www.example.com, site.example.com, and images.example.com.

In compliance with RFC 5280, the length of the domain name (technically, the Common Name) that you provide cannot exceed 64 octets (characters), including periods. To add a longer domain name, specify it in the Subject Alternative Name field, which supports names up to 253 octets in length.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `(\*\.)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])`

Required: Yes

CertificateAuthorityArn

The Amazon Resource Name (ARN) of the private certificate authority (CA) that will be used to issue the certificate. If you do not provide an ARN and you are trying to request a private certificate, ACM will attempt to issue a public certificate. For more information about private CAs, see the AWS Private Certificate Authority user guide. The ARN must have the following form:

```
arn:aws:acm-pca:region:account:certificate-
authority/12345678-1234-1234-1234-123456789012
```

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm-pca:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: No

DomainValidationOptions

The domain name that you want ACM to use to send you emails so that you can validate domain ownership.

Type: Array of DomainValidationOption objects

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Required: No

IdempotencyToken

Customer chosen string that can be used to distinguish between calls to `RequestCertificate`. Idempotency tokens time out after one hour. Therefore, if you call `RequestCertificate` multiple times with the same idempotency token within one hour, ACM recognizes that you are requesting only one certificate and will issue only one. If you change the idempotency token for each call, ACM recognizes that you are requesting multiple certificates.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 32.

Pattern: `\w+`

Required: No

KeyAlgorithm

Specifies the algorithm of the public and private key pair that your certificate uses to encrypt data. RSA is the default key algorithm for ACM certificates. Elliptic Curve Digital Signature Algorithm (ECDSA) keys are smaller, offering security comparable to RSA keys but with greater computing efficiency. However, ECDSA is not supported by all network clients. Some AWS services may require RSA keys, or only support ECDSA keys of a particular size, while others allow the use of either RSA and ECDSA keys to ensure that compatibility is not broken. Check the requirements for the AWS service where you plan to deploy your certificate. For more information about selecting an algorithm, see Key algorithms.

> **Note**
>
> Algorithms supported for an ACM certificate request include:
>
> - `RSA_2048`
> - `EC_prime256v1`
> - `EC_secp384r1`
>
> Other listed algorithms are for imported certificates only.

> **Note**
>
> When you request a private PKI certificate signed by a CA from AWS Private CA, the specified signing algorithm family (RSA or ECDSA) must match the algorithm family of the CA's secret key.

Default: RSA_2048

Type: String

Valid Values: `RSA_1024 | RSA_2048 | RSA_3072 | RSA_4096 | EC_prime256v1 | EC_secp384r1 | EC_secp521r1`

Required: No

ManagedBy

Identifies the AWS service that manages the certificate issued by ACM.

Type: String

Valid Values: `CLOUDFRONT`

Required: No

Options

You can use this parameter to specify whether to add the certificate to a certificate transparency log and export your certificate.

Certificate transparency makes it possible to detect SSL/TLS certificates that have been mistakenly or maliciously issued. Certificates that have not been logged typically produce an error message in a browser. For more information, see Opting Out of Certificate Transparency Logging.

You can export public ACM certificates to use with AWS services as well as outside the AWS Cloud. For more information, see AWS Certificate Manager exportable public certificate.

Type: CertificateOptions object

Required: No

SubjectAlternativeNames

Additional FQDNs to be included in the Subject Alternative Name extension of the ACM certificate. For example, add the name www.example.net to a certificate for which the `DomainName` field is www.example.com if users can reach your site by using either name. The maximum number of domain names that you can add to an ACM certificate is 100. However, the initial quota is 10 domain names. If you need more than 10 names, you must request a quota increase. For more information, see Quotas.

The maximum length of a SAN DNS name is 253 octets. The name is made up of multiple labels separated by periods. No label can be longer than 63 octets. Consider the following examples:

- `(63 octets).(63 octets).(63 octets).(61 octets)` is legal because the total length is 253 octets (63+1+63+1+63+1+61) and no label exceeds 63 octets.
- `(64 octets).(63 octets).(63 octets).(61 octets)` is not legal because the total length exceeds 253 octets (64+1+63+1+63+1+61) and the first label exceeds 63 octets.

- `(63 octets).(63 octets).(63 octets).(62 octets)` is not legal because the total length of the DNS name (63+1+63+1+63+1+62) exceeds 253 octets.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `(\*\.)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])`

Required: No

Tags

One or more resource tags to associate with the certificate.

Type: Array of Tag objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Required: No

ValidationMethod

The method you want to use if you are requesting a public certificate to validate that you own or control domain. You can validate with DNS or validate with email. We recommend that you use DNS validation.

Type: String

Valid Values: `EMAIL | DNS | HTTP`

Required: No

Response Syntax

```
{
   "CertificateArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CertificateArn

String that contains the ARN of the issued certificate. This must be of the form:

`arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012`

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Errors

For information about the errors that are common to all actions, see Common Error Types.

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidDomainValidationOptionsException

One or more values in the DomainValidationOption structure is incorrect.

HTTP Status Code: 400

InvalidParameterException

An input parameter was invalid.

HTTP Status Code: 400

InvalidTagException

One or both of the values that make up the key-value pair is not valid. For example, you cannot specify a tag value that begins with `aws:`.

HTTP Status Code: 400

LimitExceededException

An ACM quota has been exceeded.

HTTP Status Code: 400

TagPolicyException

A specified tag did not comply with an existing tag policy and was rejected.

HTTP Status Code: 400

TooManyTagsException

The request contains too many tags. Try the request again with fewer tags.

HTTP Status Code: 400

Examples

Request a public ACM certificate

This example illustrates one usage of RequestCertificate.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
Accept-Encoding: identity
Content-Length: 171
X-Amz-Target: CertificateManager.RequestCertificate
X-Amz-Date: 20180326T215401Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20151222/us-east-1/acm/
aws4_request,
SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
```

```
Signature=dbba4b1fa1199c011c0b781b94c97b14cbe75fa64dc6424232c903798d2a83b5

{
  "IdempotencyToken": "184627",
  "CertificateOptions": {
    "CertificateTransparencyLoggingPreference": "DISABLED"
  },
  "ValidationMethod": "DNS",
  "DomainName": "www.example.com"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 32c3ca21-3140-11e8-8ba0-f79627c5200e
Content-Type: application/x-amz-json-1.1
Content-Length: 104
Date: Mon, 26 Mar 2018 21:54:03 GMT

{
  "CertificateArn":"arn:aws:acm:us-east-1:123456789012:certificate/1ad574bd-eeb0-466e-
b961-74ec8b405093"
}
```

Request a private certificate

This example illustrates one usage of RequestCertificate.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
Accept-Encoding: identity
Content-Length: 305
X-Amz-Target: CertificateManager.RequestCertificate
X-Amz-Date: 20180331T173532Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=key_ID/20180331/us-east-1/acm/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=11be86a0995ac158327fe8ccf6f44c19af7e6768fbafe0ec10e74436770272fa

{
```

```
  "IdempotencyToken": "12563",
  "CertificateAuthorityArn": "arn:aws:acm-pca:us-east-1:account:certificate-
authority/12345678-1234-1234-1234-123456789012",
  "DomainName": "www.example.com"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: eaedc93a-3509-11e8-a99a-c76ec78904bf
Content-Type: application/x-amz-json-1.1
Content-Length: 104
Date: Sat, 31 Mar 2018 17:35:34 GMT
Connection: Keep-alive

{
  "CertificateArn": "arn:aws:acm:us-
east-1:account:certificate/88888888-4444-4444-4444-111111111111"
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ResendValidationEmail

Resends the email that requests domain ownership validation. The domain owner or an authorized representative must approve the ACM certificate before it can be issued. The certificate can be approved by clicking a link in the mail to navigate to the Amazon certificate approval website and then clicking **I Approve**. However, the validation email can be blocked by spam filters. Therefore, if you do not receive the original mail, you can request that the mail be resent within 72 hours of requesting the ACM certificate. If more than 72 hours have elapsed since your original request or since your last attempt to resend validation mail, you must request a new certificate. For more information about setting up your contact email addresses, see Configure Email for your Domain.

Request Syntax

```
{
   "CertificateArn": "string",
   "Domain": "string",
   "ValidationDomain": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

String that contains the ARN of the requested certificate. The certificate ARN is generated and returned by the RequestCertificate action as soon as the request is made. By default, using this parameter causes email to be sent to all top-level domains you specified in the certificate request. The ARN must be of the form:

`arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012`

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Domain

The fully qualified domain name (FQDN) of the certificate that needs to be validated.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `(\*\.)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])`

Required: Yes

ValidationDomain

The base validation domain that will act as the suffix of the email addresses that are used to send the emails. This must be the same as the `Domain` value or a superdomain of the `Domain` value. For example, if you requested a certificate for `site.subdomain.example.com` and specify a **ValidationDomain** of `subdomain.example.com`, ACM sends email to the the following five addresses:

- admin@subdomain.example.com
- administrator@subdomain.example.com
- hostmaster@subdomain.example.com
- postmaster@subdomain.example.com
- webmaster@subdomain.example.com

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `(\*\.)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidDomainValidationOptionsException

One or more values in the DomainValidationOption structure is incorrect.

HTTP Status Code: 400

InvalidStateException

Processing has reached an invalid state.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account or the caller's account cannot be found.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

Examples

Resend Validation Email

This example illustrates one usage of ResendValidationEmail.

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
Accept-Encoding: identity
Content-Length: 167
X-Amz-Target: CertificateManager.ResendValidationEmail
X-Amz-Date: 20151222T170722Z
User-Agent: aws-cli/1.9.7 Python/2.7.3 Linux/3.13.0-73-generic botocore/1.3.7
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=key_ID/20151222/us-east-1/acm/aws4_request,
SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=7ec7e70cd614724945545b22bc28296f77803d0c2524573d41c994668f07f435

{
  "CertificateArn": "arn:aws:acm:us-
east-1:111122223333 :certificate/12345678-1234-1234-1234-1234567890912",
  "Domain": "www.example.com",
  "ValidationDomain": "example.com"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 74bada6d-a8ce-11e5-82ad-d565a2aaa0b3
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Date: Tue, 22 Dec 2015 17:07:18 GMT
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

RevokeCertificate

Revokes a public ACM certificate. You can only revoke certificates that have been previously exported.

> **Important**
>
> Once a certificate is revoked, you cannot reuse the certificate. Revoking a certificate is permanent.

Request Syntax

```
{
   "CertificateArn": "string",
   "RevocationReason": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

The Amazon Resource Name (ARN) of the public or private certificate that will be revoked. The ARN must have the following form:

`arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012`

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

RevocationReason

Specifies why you revoked the certificate.

Type: String

Valid Values: `UNSPECIFIED | KEY_COMPROMISE | CA_COMPROMISE | AFFILIATION_CHANGED | SUPERCEDED | SUPERSEDED | CESSATION_OF_OPERATION | CERTIFICATE_HOLD | REMOVE_FROM_CRL | PRIVILEGE_WITHDRAWN | A_A_COMPROMISE`

Required: Yes

Response Syntax

```
{
   "CertificateArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CertificateArn

The Amazon Resource Name (ARN) of the public or private certificate that was revoked.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

You do not have access required to perform this action.

HTTP Status Code: 400

ConflictException

You are trying to update a resource or configuration that is already being created or updated. Wait for the previous operation to finish and try again.

HTTP Status Code: 400

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

ResourceInUseException

The certificate is in use by another AWS service in the caller's account. Remove the association and try again.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account or the caller's account cannot be found.

HTTP Status Code: 400

ThrottlingException

The request was denied because it exceeded a quota.

throttlingReasons

One or more reasons why the request was throttled.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

SearchCertificates

Retrieves a list of certificates matching search criteria. You can filter certificates by X.509 attributes and ACM specific properties like certificate status, type and renewal eligibility. This operation provides more flexible filtering than ListCertificates by supporting complex filter statements.

Request Syntax

```
{
   "FilterStatement": { ... },
   "MaxResults": number,
   "NextToken": "string",
   "SortBy": "string",
   "SortOrder": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

FilterStatement

A filter statement that defines the search criteria. You can combine multiple filters using AND, OR, and NOT logical operators to create complex queries.

Type: CertificateFilterStatement object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

MaxResults

The maximum number of results to return in the response. Default is 100.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 500.

Required: No

NextToken

Use this parameter only when paginating results and only in a subsequent request after you receive a response with truncated results. Set it to the value of `NextToken` from the response you just received.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10000.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Required: No

SortBy

Specifies the field to sort results by. Valid values are CREATED_AT, NOT_AFTER, STATUS, RENEWAL_STATUS, EXPORTED, IN_USE, NOT_BEFORE, KEY_ALGORITHM, TYPE, CERTIFICATE_ARN, COMMON_NAME, REVOKED_AT, RENEWAL_ELIGIBILITY, ISSUED_AT, MANAGED_BY, EXPORT_OPTION, VALIDATION_METHOD, and IMPORTED_AT.

Type: String

Valid Values: `CREATED_AT | NOT_AFTER | STATUS | RENEWAL_STATUS | EXPORTED | IN_USE | NOT_BEFORE | KEY_ALGORITHM | TYPE | CERTIFICATE_ARN | COMMON_NAME | REVOKED_AT | RENEWAL_ELIGIBILITY | ISSUED_AT | MANAGED_BY | EXPORT_OPTION | VALIDATION_METHOD | IMPORTED_AT`

Required: No

SortOrder

Specifies the order of sorted results. Valid values are ASCENDING or DESCENDING.

Type: String

Valid Values: `ASCENDING | DESCENDING`

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "Results": [
      {
         "CertificateArn": "string",
         "CertificateMetadata": { ... },
         "X509Attributes": {
            "ExtendedKeyUsages": [ "string" ],
            "Issuer": {
               "CommonName": "string",
               "Country": "string",
               "CustomAttributes": [
                  {
                     "ObjectIdentifier": "string",
                     "Value": "string"
                  }
               ],
               "DistinguishedNameQualifier": "string",
               "DomainComponents": [ "string" ],
               "GenerationQualifier": "string",
               "GivenName": "string",
               "Initials": "string",
               "Locality": "string",
               "Organization": "string",
               "OrganizationalUnit": "string",
               "Pseudonym": "string",
               "SerialNumber": "string",
               "State": "string",
               "Surname": "string",
               "Title": "string"
            },
            "KeyAlgorithm": "string",
            "KeyUsages": [ "string" ],
            "NotAfter": number,
            "NotBefore": number,
            "SerialNumber": "string",
            "Subject": {
               "CommonName": "string",
               "Country": "string",
               "CustomAttributes": [
                  {
```

```
                    "ObjectIdentifier": "string",
                    "Value": "string"
                 }
              ],
              "DistinguishedNameQualifier": "string",
              "DomainComponents": [ "string" ],
              "GenerationQualifier": "string",
              "GivenName": "string",
              "Initials": "string",
              "Locality": "string",
              "Organization": "string",
              "OrganizationalUnit": "string",
              "Pseudonym": "string",
              "SerialNumber": "string",
              "State": "string",
              "Surname": "string",
              "Title": "string"
           },
           "SubjectAlternativeNames": [
              { ... }
           ]
        }
     }
  ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken

When the list is truncated, this value is present and contains the value to use for the `NextToken` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10000.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Results

A list of certificate search results containing certificate ARNs, X.509 attributes, and ACM metadata.

Type: Array of CertificateSearchResult objects

Errors

For information about the errors that are common to all actions, see Common Error Types.

AccessDeniedException

You do not have access required to perform this action.

HTTP Status Code: 400

ThrottlingException

The request was denied because it exceeded a quota.

throttlingReasons

One or more reasons why the request was throttled.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

Examples

Search Certificates

The following example searches for exported, issued certificates that are either imported or private, excluding a specific domain name.

Sample Request

```
POST / HTTP/1.1
```

```
Host: acm.us-east-1.amazonaws.com
Accept-Encoding: identity
Content-Length: 450
X-Amz-Target: CertificateManager.SearchCertificates
X-Amz-Date: 20260213T034622Z
User-Agent: aws-cli/2.0.0 Python/3.9.0 Linux/5.10.0
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=key_ID/20260213/us-east-1/acm/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=example...

{
    "FilterStatement": {
        "And": [
            {
                "Filter": {
                    "AcmCertificateMetadataFilter": {
                        "Status": "ISSUED"
                    }
                }
            },
            {
                "Or": [
                    {
                        "Filter": {
                            "AcmCertificateMetadataFilter": {
                                "Type": "IMPORTED"
                            }
                        }
                    },
                    {
                        "Filter": {
                            "AcmCertificateMetadataFilter": {
                                "Type": "PRIVATE"
                            }
                        }
                    }
                ]
            },
            {
                "Not": {
                    "Filter": {
                        "X509AttributeFilter": {
                            "SubjectAlternativeName": {
```

```
                                "DnsName": {
                                    "Value": "test.com",
                                    "ComparisonOperator": "CONTAINS"
                                }
                            }
                        }
                    }
                },
                {
                    "Filter": {
                        "AcmCertificateMetadataFilter": {
                            "Exported": true
                        }
                    }
                }
            ]
        },
        "MaxResults": 10,
        "SortBy": "CREATED_AT",
        "SortOrder": "DESCENDING"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 12345678-1234-1234-1234-123456789012
Content-Type: application/x-amz-json-1.1
Content-Length: 500
Date: Fri, 13 Feb 2026 03:46:22 GMT
Connection: Keep-alive

{
    "Results": [
        {
            "CertificateArn":
 "arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012",
            "X509Attributes": {
                "Issuer": {
                    "CommonName": "Example CA",
                    "Country": "US",
                    "Organization": "Example Corp"
```

```
                },
                "Subject": {
                    "CommonName": "www.example.com"
                },
                "ExtendedKeyUsages": [
                    "TLS_WEB_SERVER_AUTHENTICATION"
                ],
                "KeyAlgorithm": "RSA_2048",
                "KeyUsages": [
                    "DIGITAL_SIGNATURE"
                ],
                "SerialNumber": "e5:87:ef:34:7a:4a:0f:de",
                "NotAfter": "2028-12-31T23:59:59+00:00",
                "NotBefore": "2008-01-01T00:00:01+00:00"
            },
            "CertificateMetadata": {
                "AcmCertificateMetadata": {
                    "CreatedAt": "2020-06-15T18:47:09+00:00",
                    "Exported": true,
                    "ImportedAt": "2020-06-15T18:47:09+00:00",
                    "InUse": true,
                    "RenewalEligibility": "INELIGIBLE",
                    "Status": "ISSUED",
                    "Type": "IMPORTED",
                    "ExportOption": "DISABLED"
                }
            }
        }
    ],
    "NextToken": "nextToken"
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateCertificateOptions

Updates a certificate. You can use this function to specify whether to opt in to or out of recording your certificate in a certificate transparency log and exporting. For more information, see Opting Out of Certificate Transparency Logging and AWS Certificate Manager Exportable Managed Certificates.

Request Syntax

```
{
   "CertificateArn": "string",
   "Options": {
      "CertificateTransparencyLoggingPreference": "string",
      "Export": "string"
   }
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters.

The request accepts the following data in JSON format.

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

ARN of the requested certificate to update. This must be of the form:

`arn:aws:acm:us-east-1:`*`account`*`:certificate/`*`12345678-1234-1234-1234-123456789012`*

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: Yes

Options

Use to update the options for your certificate. Currently, you can specify whether to add your certificate to a transparency log or export your certificate. Certificate transparency makes it possible to detect SSL/TLS certificates that have been mistakenly or maliciously issued. Certificates that have not been logged typically produce an error message in a browser.

Type: CertificateOptions object

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Error Types.

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidStateException

Processing has reached an invalid state.

HTTP Status Code: 400

LimitExceededException

An ACM quota has been exceeded.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account or the caller's account cannot be found.

HTTP Status Code: 400

ValidationException

The supplied input failed to satisfy constraints of an AWS service.

HTTP Status Code: 400

Examples

UpdateCertificateOptions

This example illustrates one usage of UpdateCertificateOptions.

Sample Request

```
POST / HTTP/1.1
acm.us-east-1.amazonaws.com
Accept-Encoding: identity
Content-Length: 185
X-Amz-Target: CertificateManager.UpdateCertificateOptions
X-Amz-Date: 20180326T222032Z
User-Agent: aws-cli/1.14.28 Python/2.7.9 Windows/8 botocore/1.8.32
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=key_ID/20151222/us-east-1/acm/aws4_request,
SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=7ec7e70cd614724945545b22bc28296f77803d0c2524573d41c994668f07f435

{
  "CertificateArn":
 "arn:aws:acm:region:account:certificate/12345678-1234-1234-1234-123456789012",
  "CertificateOptions": {
    "CertificateTransparencyLoggingPreference": "DISABLED"
  }
}
```

Example

This example illustrates one usage of UpdateCertificateOptions.

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: e6f55ecb-3143-11e8-af72-0bd5049841d5
```

```
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Date: Tue, 22 Dec 2015 17:07:18 GMT
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Data Types

The AWS Certificate Manager API contains several data types that various actions use. This section describes each data type in detail.

> **Note**
>
> The order of each element in a data type structure is not guaranteed. Applications should not assume a particular order.

The following data types are supported:

- AcmCertificateMetadata
- AcmCertificateMetadataFilter
- CertificateDetail
- CertificateFilter
- CertificateFilterStatement
- CertificateMetadata
- CertificateOptions
- CertificateSearchResult
- CertificateSummary
- CommonNameFilter
- CustomAttribute
- DistinguishedName
- DnsNameFilter
- DomainValidation
- DomainValidationOption
- ExpiryEventsConfiguration
- ExtendedKeyUsage
- Filters
- GeneralName
- HttpRedirect

- KeyUsage
- OtherName
- RenewalSummary
- ResourceRecord
- SubjectAlternativeNameFilter
- SubjectFilter
- Tag
- ThrottlingReason
- TimestampRange
- X509AttributeFilter
- X509Attributes

AcmCertificateMetadata

Contains ACM-specific metadata about a certificate.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

CreatedAt

The time at which the certificate was requested.

Type: Timestamp

Required: No

Exported

Indicates whether the certificate has been exported.

Type: Boolean

Required: No

ExportOption

Indicates whether the certificate can be exported.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

ImportedAt

The date and time when the certificate was imported. This value exists only when the certificate type is `IMPORTED`.

Type: Timestamp

Required: No

InUse

Indicates whether the certificate is currently in use by an AWS service.

Type: Boolean

Required: No

IssuedAt

The time at which the certificate was issued. This value exists only when the certificate type is `AMAZON_ISSUED`.

Type: Timestamp

Required: No

ManagedBy

Identifies the AWS service that manages the certificate issued by ACM.

Type: String

Valid Values: `CLOUDFRONT`

Required: No

RenewalEligibility

Specifies whether the certificate is eligible for renewal. At this time, only exported private certificates can be renewed with the RenewCertificate command.

Type: String

Valid Values: `ELIGIBLE | INELIGIBLE`

Required: No

RenewalStatus

The renewal status of the certificate.

Type: String

Valid Values: `PENDING_AUTO_RENEWAL | PENDING_VALIDATION | SUCCESS | FAILED`

Required: No

RevokedAt

The time at which the certificate was revoked. This value exists only when the certificate status is REVOKED.

Type: Timestamp

Required: No

Status

The status of the certificate.

A certificate enters status PENDING_VALIDATION upon being requested, unless it fails for any of the reasons given in the troubleshooting topic Certificate request fails. ACM makes repeated attempts to validate a certificate for 72 hours and then times out. If a certificate shows status FAILED or VALIDATION_TIMED_OUT, delete the request, correct the issue with DNS validation or Email validation, and try again. If validation succeeds, the certificate enters status ISSUED.

Type: String

Valid Values: `PENDING_VALIDATION | ISSUED | INACTIVE | EXPIRED | VALIDATION_TIMED_OUT | REVOKED | FAILED`

Required: No

Type

The source of the certificate. For certificates provided by ACM, this value is AMAZON_ISSUED. For certificates that you imported with ImportCertificate, this value is IMPORTED. ACM does not provide managed renewal for imported certificates. For more information about the differences between certificates that you import and those that ACM provides, see Importing Certificates in the *AWS Certificate Manager User Guide*.

Type: String

Valid Values: `IMPORTED | AMAZON_ISSUED | PRIVATE`

Required: No

ValidationMethod

Specifies the domain validation method.

Type: String

Valid Values: `EMAIL | DNS | HTTP`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AcmCertificateMetadataFilter

Filters certificates by ACM metadata.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

> **Important**
>
> This data type is a UNION, so only one of the following members can be specified when used or returned.

Exported

Filter by whether the certificate has been exported.

Type: Boolean

Required: No

ExportOption

Filter by certificate export option.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

InUse

Filter by whether the certificate is in use.

Type: Boolean

Required: No

ManagedBy

Filter by the entity that manages the certificate.

Type: String

Valid Values: `CLOUDFRONT`

Required: No

RenewalStatus

Filter by certificate renewal status.

Type: String

Valid Values: `PENDING_AUTO_RENEWAL | PENDING_VALIDATION | SUCCESS | FAILED`

Required: No

Status

Filter by certificate status.

Type: String

Valid Values: `PENDING_VALIDATION | ISSUED | INACTIVE | EXPIRED | VALIDATION_TIMED_OUT | REVOKED | FAILED`

Required: No

Type

Filter by certificate type.

Type: String

Valid Values: `IMPORTED | AMAZON_ISSUED | PRIVATE`

Required: No

ValidationMethod

Filter by validation method.

Type: String

Valid Values: `EMAIL | DNS | HTTP`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CertificateDetail

Contains metadata about an ACM certificate. This structure is returned in the response to a DescribeCertificate request.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

The Amazon Resource Name (ARN) of the certificate. For more information about ARNs, see Amazon Resource Names (ARNs) in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: No

CertificateAuthorityArn

The Amazon Resource Name (ARN) of the private certificate authority (CA) that issued the certificate. This has the following format:

`arn:aws:acm-pca:region:account:certificate-authority/12345678-1234-1234-1234-123456789012`

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: No

CreatedAt

The time at which the certificate was requested.

Type: Timestamp

Required: No

DomainName

The fully qualified domain name for the certificate, such as www.example.com or example.com.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `(\*\.)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])`

Required: No

DomainValidationOptions

Contains information about the initial validation of each domain name that occurs as a result of the RequestCertificate request. This field exists only when the certificate type is `AMAZON_ISSUED`.

Type: Array of DomainValidation objects

Array Members: Minimum number of 1 item. Maximum number of 1000 items.

Required: No

ExtendedKeyUsages

Contains a list of Extended Key Usage X.509 v3 extension objects. Each object specifies a purpose for which the certificate public key can be used and consists of a name and an object identifier (OID).

Type: Array of ExtendedKeyUsage objects

Required: No

FailureReason

The reason the certificate request failed. This value exists only when the certificate status is `FAILED`. For more information, see Certificate Request Failed in the *AWS Certificate Manager User Guide*.

Type: String

Valid Values: `NO_AVAILABLE_CONTACTS | ADDITIONAL_VERIFICATION_REQUIRED | DOMAIN_NOT_ALLOWED | INVALID_PUBLIC_DOMAIN | DOMAIN_VALIDATION_DENIED | CAA_ERROR | PCA_LIMIT_EXCEEDED | PCA_INVALID_ARN | PCA_INVALID_STATE | PCA_REQUEST_FAILED | PCA_NAME_CONSTRAINTS_VALIDATION | PCA_RESOURCE_NOT_FOUND | PCA_INVALID_ARGS | PCA_INVALID_DURATION | PCA_ACCESS_DENIED | SLR_NOT_FOUND | OTHER`

Required: No

ImportedAt

The date and time when the certificate was imported. This value exists only when the certificate type is `IMPORTED`.

Type: Timestamp

Required: No

InUseBy

A list of ARNs for the AWS resources that are using the certificate. A certificate can be used by multiple AWS resources.

Type: Array of strings

Required: No

IssuedAt

The time at which the certificate was issued. This value exists only when the certificate type is `AMAZON_ISSUED`.

Type: Timestamp

Required: No

Issuer

The name of the certificate authority that issued and signed the certificate.

Type: String

Required: No

KeyAlgorithm

The algorithm that was used to generate the public-private key pair.

Type: String

Valid Values: `RSA_1024 | RSA_2048 | RSA_3072 | RSA_4096 | EC_prime256v1 | EC_secp384r1 | EC_secp521r1`

Required: No

KeyUsages

A list of Key Usage X.509 v3 extension objects. Each object is a string value that identifies the purpose of the public key contained in the certificate. Possible extension values include DIGITAL_SIGNATURE, KEY_ENCHIPHERMENT, NON_REPUDIATION, and more.

Type: Array of KeyUsage objects

Required: No

ManagedBy

Identifies the AWS service that manages the certificate issued by ACM.

Type: String

Valid Values: `CLOUDFRONT`

Required: No

NotAfter

The time after which the certificate is not valid.

Type: Timestamp

Required: No

NotBefore

The time before which the certificate is not valid.

Type: Timestamp

Required: No

Options

Value that specifies whether to add the certificate to a transparency log. Certificate transparency makes it possible to detect SSL certificates that have been mistakenly or maliciously issued. A browser might respond to certificate that has not been logged by showing an error message. The logs are cryptographically secure.

Type: CertificateOptions object

Required: No

RenewalEligibility

Specifies whether the certificate is eligible for renewal. At this time, only exported private certificates can be renewed with the RenewCertificate command.

Type: String

Valid Values: `ELIGIBLE | INELIGIBLE`

Required: No

RenewalSummary

Contains information about the status of ACM's managed renewal for the certificate. This field exists only when the certificate type is `AMAZON_ISSUED`.

Type: RenewalSummary object

Required: No

RevocationReason

The reason the certificate was revoked. This value exists only when the certificate status is `REVOKED`.

Type: String

Valid Values: `UNSPECIFIED | KEY_COMPROMISE | CA_COMPROMISE | AFFILIATION_CHANGED | SUPERCEDED | SUPERSEDED | CESSATION_OF_OPERATION | CERTIFICATE_HOLD | REMOVE_FROM_CRL | PRIVILEGE_WITHDRAWN | A_A_COMPROMISE`

Required: No

RevokedAt

The time at which the certificate was revoked. This value exists only when the certificate status is `REVOKED`.

Type: Timestamp

Required: No

Serial

The serial number of the certificate.

Type: String

Required: No

SignatureAlgorithm

The algorithm that was used to sign the certificate.

Type: String

Required: No

Status

The status of the certificate.

A certificate enters status PENDING_VALIDATION upon being requested, unless it fails for any of the reasons given in the troubleshooting topic Certificate request fails. ACM makes repeated attempts to validate a certificate for 72 hours and then times out. If a certificate shows status FAILED or VALIDATION_TIMED_OUT, delete the request, correct the issue with DNS validation or Email validation, and try again. If validation succeeds, the certificate enters status ISSUED.

Type: String

Valid Values: `PENDING_VALIDATION | ISSUED | INACTIVE | EXPIRED | VALIDATION_TIMED_OUT | REVOKED | FAILED`

Required: No

Subject

The name of the entity that is associated with the public key contained in the certificate.

Type: String

Required: No

SubjectAlternativeNames

One or more domain names (subject alternative names) included in the certificate. This list contains the domain names that are bound to the public key that is contained in the certificate. The subject alternative names include the canonical domain name (CN) of the certificate and additional domain names that can be used to connect to the website.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `(\*\.)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])`

Required: No

Type

The source of the certificate. For certificates provided by ACM, this value is `AMAZON_ISSUED`. For certificates that you imported with ImportCertificate, this value is `IMPORTED`. ACM does not provide managed renewal for imported certificates. For more information about the differences between certificates that you import and those that ACM provides, see Importing Certificates in the *AWS Certificate Manager User Guide*.

Type: String

Valid Values: `IMPORTED | AMAZON_ISSUED | PRIVATE`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CertificateFilter

Defines a filter for searching certificates by ARN, X.509 attributes, or ACM metadata.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

> **Important**
>
> This data type is a UNION, so only one of the following members can be specified when used or returned.

AcmCertificateMetadataFilter

Filter by ACM certificate metadata.

Type: AcmCertificateMetadataFilter object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

CertificateArn

Filter by certificate ARN.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: No

X509AttributeFilter

Filter by X.509 certificate attributes.

Type: X509AttributeFilter object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CertificateFilterStatement

A filter statement used to search for certificates. Can contain AND, OR, NOT logical operators or a single filter.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

> **Important**
>
> This data type is a UNION, so only one of the following members can be specified when used or returned.

And

A list of filter statements that must all be true.

Type: Array of CertificateFilterStatement objects

Array Members: Minimum number of 1 item. Maximum number of 15 items.

Required: No

Filter

A single certificate filter.

Type: CertificateFilter object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

Not

A filter statement that must not be true.

Type: CertificateFilterStatement object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

Or

A list of filter statements where at least one must be true.

Type: Array of CertificateFilterStatement objects

Array Members: Minimum number of 1 item. Maximum number of 15 items.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CertificateMetadata

Contains metadata about a certificate. Currently supports ACM certificate metadata.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

> **Important**
>
> This data type is a UNION, so only one of the following members can be specified when used or returned.

AcmCertificateMetadata

Metadata for an ACM certificate.

Type: AcmCertificateMetadata object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CertificateOptions

Structure that contains options for your certificate. You can use this structure to specify whether to opt in to or out of certificate transparency logging and export your certificate.

Some browsers require that public certificates issued for your domain be recorded in a log. Certificates that are not logged typically generate a browser error. Transparency makes it possible for you to detect SSL/TLS certificates that have been mistakenly or maliciously issued for your domain. For general information, see Certificate Transparency Logging.

You can export public ACM certificates to use with AWS services as well as outside AWS Cloud. For more information, see AWS Certificate Manager exportable public certificate.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

CertificateTransparencyLoggingPreference

You can opt out of certificate transparency logging by specifying the `DISABLED` option. Opt in by specifying `ENABLED`.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

Export

You can opt in to allow the export of your certificates by specifying `ENABLED`. You cannot update the value of `Export` after the the certificate is created.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CertificateSearchResult

Contains information about a certificate returned by the SearchCertificates action. This structure includes the certificate ARN, X.509 attributes, and ACM metadata.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

The Amazon Resource Name (ARN) of the certificate.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: No

CertificateMetadata

ACM-specific metadata about the certificate.

Type: CertificateMetadata object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

X509Attributes

X.509 certificate attributes such as subject, issuer, and validity period.

Type: X509Attributes object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CertificateSummary

This structure is returned in the response object of ListCertificates action.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

CertificateArn

Amazon Resource Name (ARN) of the certificate. This is of the form:

`arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789`

For more information about ARNs, see Amazon Resource Names (ARNs).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/,.@-]+:acm:[\w+=/,.@-]*:[0-9]+:[\w+=,.@-]+(/[\w+=,.@-]+)*`

Required: No

CreatedAt

The time at which the certificate was requested.

Type: Timestamp

Required: No

DomainName

Fully qualified domain name (FQDN), such as www.example.com or example.com, for the certificate.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `(\*\.)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])`

Required: No

Exported

Indicates whether the certificate has been exported. This value exists only when the certificate type is `PRIVATE`.

Type: Boolean

Required: No

ExportOption

Indicates if export is enabled for the certificate.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

ExtendedKeyUsages

Contains a list of Extended Key Usage X.509 v3 extension objects. Each object specifies a purpose for which the certificate public key can be used and consists of a name and an object identifier (OID).

Type: Array of strings

Valid Values: `TLS_WEB_SERVER_AUTHENTICATION | TLS_WEB_CLIENT_AUTHENTICATION | CODE_SIGNING | EMAIL_PROTECTION | TIME_STAMPING | OCSP_SIGNING | IPSEC_END_SYSTEM | IPSEC_TUNNEL | IPSEC_USER | ANY | NONE | CUSTOM`

Required: No

HasAdditionalSubjectAlternativeNames

When called by ListCertificates, indicates whether the full list of subject alternative names has been included in the response. If false, the response includes all of the subject alternative

names included in the certificate. If true, the response only includes the first 100 subject alternative names included in the certificate. To display the full list of subject alternative names, use DescribeCertificate.

Type: Boolean

Required: No

ImportedAt

The date and time when the certificate was imported. This value exists only when the certificate type is `IMPORTED`.

Type: Timestamp

Required: No

InUse

Indicates whether the certificate is currently in use by any AWS resources.

Type: Boolean

Required: No

IssuedAt

The time at which the certificate was issued. This value exists only when the certificate type is `AMAZON_ISSUED`.

Type: Timestamp

Required: No

KeyAlgorithm

The algorithm that was used to generate the public-private key pair.

Type: String

Valid Values: `RSA_1024 | RSA_2048 | RSA_3072 | RSA_4096 | EC_prime256v1 | EC_secp384r1 | EC_secp521r1`

Required: No

KeyUsages

A list of Key Usage X.509 v3 extension objects. Each object is a string value that identifies the purpose of the public key contained in the certificate. Possible extension values include DIGITAL_SIGNATURE, KEY_ENCHIPHERMENT, NON_REPUDIATION, and more.

Type: Array of strings

Valid Values: `DIGITAL_SIGNATURE | NON_REPUDIATION | KEY_ENCIPHERMENT | DATA_ENCIPHERMENT | KEY_AGREEMENT | CERTIFICATE_SIGNING | CRL_SIGNING | ENCIPHER_ONLY | DECIPHER_ONLY | ANY | CUSTOM`

Required: No

ManagedBy

Identifies the AWS service that manages the certificate issued by ACM.

Type: String

Valid Values: `CLOUDFRONT`

Required: No

NotAfter

The time after which the certificate is not valid.

Type: Timestamp

Required: No

NotBefore

The time before which the certificate is not valid.

Type: Timestamp

Required: No

RenewalEligibility

Specifies whether the certificate is eligible for renewal. At this time, only exported private certificates can be renewed with the RenewCertificate command.

Type: String

Valid Values: `ELIGIBLE | INELIGIBLE`

Required: No

RevokedAt

The time at which the certificate was revoked. This value exists only when the certificate status is `REVOKED`.

Type: Timestamp

Required: No

Status

The status of the certificate.

A certificate enters status PENDING_VALIDATION upon being requested, unless it fails for any of the reasons given in the troubleshooting topic Certificate request fails. ACM makes repeated attempts to validate a certificate for 72 hours and then times out. If a certificate shows status FAILED or VALIDATION_TIMED_OUT, delete the request, correct the issue with DNS validation or Email validation, and try again. If validation succeeds, the certificate enters status ISSUED.

Type: String

Valid Values: `PENDING_VALIDATION | ISSUED | INACTIVE | EXPIRED | VALIDATION_TIMED_OUT | REVOKED | FAILED`

Required: No

SubjectAlternativeNameSummaries

One or more domain names (subject alternative names) included in the certificate. This list contains the domain names that are bound to the public key that is contained in the certificate. The subject alternative names include the canonical domain name (CN) of the certificate and additional domain names that can be used to connect to the website.

When called by ListCertificates, this parameter will only return the first 100 subject alternative names included in the certificate. To display the full list of subject alternative names, use DescribeCertificate.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `(\*\.)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])`

Required: No

Type

The source of the certificate. For certificates provided by ACM, this value is `AMAZON_ISSUED`. For certificates that you imported with ImportCertificate, this value is `IMPORTED`. ACM does not provide managed renewal for imported certificates. For more information about the differences between certificates that you import and those that ACM provides, see Importing Certificates in the *AWS Certificate Manager User Guide*.

Type: String

Valid Values: `IMPORTED | AMAZON_ISSUED | PRIVATE`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CommonNameFilter

Filters certificates by common name.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

ComparisonOperator

The comparison operator to use.

Type: String

Valid Values: `CONTAINS | EQUALS`

Required: Yes

Value

The value to match against.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CustomAttribute

Defines the X.500 relative distinguished name (RDN).

Contents

> **Note**
>
> In the following list, the required parameters are described first.

ObjectIdentifier

Specifies the object identifier (OID) of the attribute type of the relative distinguished name (RDN).

Type: String

Required: No

Value

Specifies the attribute value of relative distinguished name (RDN).

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DistinguishedName

Contains X.500 distinguished name information.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

CommonName

The common name (CN) attribute.

Type: String

Required: No

Country

The country (C) attribute.

Type: String

Required: No

CustomAttributes

A list of custom attributes in the distinguished name. Each custom attribute contains an object identifier (OID) and its corresponding value.

Type: Array of CustomAttribute objects

Required: No

DistinguishedNameQualifier

The distinguished name qualifier attribute.

Type: String

Required: No

DomainComponents

The domain component attributes.

Type: Array of strings

Required: No

GenerationQualifier

The generation qualifier attribute.

Type: String

Required: No

GivenName

The given name attribute.

Type: String

Required: No

Initials

The initials attribute.

Type: String

Required: No

Locality

The locality (L) attribute.

Type: String

Required: No

Organization

The organization (O) attribute.

Type: String

Required: No

OrganizationalUnit

The organizational unit (OU) attribute.

Type: String

Required: No

Pseudonym

The pseudonym attribute.

Type: String

Required: No

SerialNumber

The serial number attribute.

Type: String

Required: No

State

The state or province (ST) attribute.

Type: String

Required: No

Surname

The surname attribute.

Type: String

Required: No

Title

The title attribute.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DnsNameFilter

Filters certificates by DNS name.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

ComparisonOperator

The comparison operator to use.

Type: String

Valid Values: `CONTAINS | EQUALS`

Required: Yes

Value

The DNS name value to match against.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DomainValidation

Contains information about the validation of each domain name in the certificate.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

DomainName

A fully qualified domain name (FQDN) in the certificate. For example, `www.example.com` or `example.com`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `(\*\.)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])`

Required: Yes

HttpRedirect

Contains information for HTTP-based domain validation of certificates requested through Amazon CloudFront and issued by ACM. This field exists only when the certificate type is `AMAZON_ISSUED` and the validation method is `HTTP`.

Type: HttpRedirect object

Required: No

ResourceRecord

Contains the CNAME record that you add to your DNS database for domain validation. For more information, see Use DNS to Validate Domain Ownership.

> **Note**
>
> The CNAME information that you need does not include the name of your domain. If you include your domain name in the DNS database CNAME record, validation fails. For example, if the name is `_a79865eb4cd1a6ab990a45779b4e0b96.yourdomain.com`, only `_a79865eb4cd1a6ab990a45779b4e0b96` must be used.

Type: ResourceRecord object

Required: No

ValidationDomain

The domain name that ACM used to send domain validation emails.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `(\*\.)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])`

Required: No

ValidationEmails

A list of email addresses that ACM used to send domain validation emails.

Type: Array of strings

Required: No

ValidationMethod

Specifies the domain validation method.

Type: String

Valid Values: `EMAIL | DNS | HTTP`

Required: No

ValidationStatus

The validation status of the domain name. This can be one of the following values:

- PENDING_VALIDATION
- SUCCESS
- FAILED

Type: String

Valid Values: PENDING_VALIDATION | SUCCESS | FAILED

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DomainValidationOption

Contains information about the domain names that you want ACM to use to send you emails that enable you to validate domain ownership.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

DomainName

A fully qualified domain name (FQDN) in the certificate request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `(\*\.)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])`

Required: Yes

ValidationDomain

The domain name that you want ACM to use to send you validation emails. This domain name is the suffix of the email addresses that you want ACM to use. This must be the same as the `DomainName` value or a superdomain of the `DomainName` value. For example, if you request a certificate for `testing.example.com`, you can specify `example.com` for this value. In that case, ACM sends domain validation emails to the following five addresses:

- admin@example.com
- administrator@example.com
- hostmaster@example.com
- postmaster@example.com
- webmaster@example.com

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `(\*\.)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ExpiryEventsConfiguration

Object containing expiration events options associated with an AWS account.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

DaysBeforeExpiry

Specifies the number of days prior to certificate expiration when ACM starts generating `EventBridge` events. ACM sends one event per day per certificate until the certificate expires. By default, accounts receive events starting 45 days before certificate expiration.

Type: Integer

Valid Range: Minimum value of 1.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ExtendedKeyUsage

The Extended Key Usage X.509 v3 extension defines one or more purposes for which the public key can be used. This is in addition to or in place of the basic purposes specified by the Key Usage extension.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

Name

The name of an Extended Key Usage value.

Type: String

Valid Values: `TLS_WEB_SERVER_AUTHENTICATION | TLS_WEB_CLIENT_AUTHENTICATION | CODE_SIGNING | EMAIL_PROTECTION | TIME_STAMPING | OCSP_SIGNING | IPSEC_END_SYSTEM | IPSEC_TUNNEL | IPSEC_USER | ANY | NONE | CUSTOM`

Required: No

OID

An object identifier (OID) for the extension value. OIDs are strings of numbers separated by periods. The following OIDs are defined in RFC 3280 and RFC 5280.

- `1.3.6.1.5.5.7.3.1 (TLS_WEB_SERVER_AUTHENTICATION)`
- `1.3.6.1.5.5.7.3.2 (TLS_WEB_CLIENT_AUTHENTICATION)`
- `1.3.6.1.5.5.7.3.3 (CODE_SIGNING)`
- `1.3.6.1.5.5.7.3.4 (EMAIL_PROTECTION)`
- `1.3.6.1.5.5.7.3.8 (TIME_STAMPING)`
- `1.3.6.1.5.5.7.3.9 (OCSP_SIGNING)`
- `1.3.6.1.5.5.7.3.5 (IPSEC_END_SYSTEM)`
- `1.3.6.1.5.5.7.3.6 (IPSEC_TUNNEL)`
- `1.3.6.1.5.5.7.3.7 (IPSEC_USER)`

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Filters

This structure can be used in the ListCertificates action to filter the output of the certificate list.

Contents

> **Note**
> In the following list, the required parameters are described first.

exportOption

Specify ENABLED or DISABLED to identify certificates that can be exported.

Type: String

Valid Values: ENABLED | DISABLED

Required: No

extendedKeyUsage

Specify one or more ExtendedKeyUsage extension values.

Type: Array of strings

Valid Values: TLS_WEB_SERVER_AUTHENTICATION | TLS_WEB_CLIENT_AUTHENTICATION | CODE_SIGNING | EMAIL_PROTECTION | TIME_STAMPING | OCSP_SIGNING | IPSEC_END_SYSTEM | IPSEC_TUNNEL | IPSEC_USER | ANY | NONE | CUSTOM

Required: No

keyTypes

Specify one or more algorithms that can be used to generate key pairs.

Default filtering returns only RSA_1024 and RSA_2048 certificates that have at least one domain. To return other certificate types, provide the desired type signatures in a comma-separated list. For example, "keyTypes": ["RSA_2048","RSA_4096"] returns both RSA_2048 and RSA_4096 certificates.

Type: Array of strings

Valid Values: `RSA_1024 | RSA_2048 | RSA_3072 | RSA_4096 | EC_prime256v1 | EC_secp384r1 | EC_secp521r1`

Required: No

keyUsage

Specify one or more KeyUsage extension values.

Type: Array of strings

Valid Values: `DIGITAL_SIGNATURE | NON_REPUDIATION | KEY_ENCIPHERMENT | DATA_ENCIPHERMENT | KEY_AGREEMENT | CERTIFICATE_SIGNING | CRL_SIGNING | ENCIPHER_ONLY | DECIPHER_ONLY | ANY | CUSTOM`

Required: No

managedBy

Identifies the AWS service that manages the certificate issued by ACM.

Type: String

Valid Values: `CLOUDFRONT`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

GeneralName

Describes an ASN.1 X.400 `GeneralName` as defined in RFC 5280. Only one of the following naming options should be provided.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

> **Important**
>
> This data type is a UNION, so only one of the following members can be specified when used or returned.

DirectoryName

Contains information about the certificate subject. The `Subject` field in the certificate identifies the entity that owns or controls the public key in the certificate. The entity can be a user, computer, device, or service. The `Subject` must contain an X.500 distinguished name (DN). A DN is a sequence of relative distinguished names (RDNs). The RDNs are separated by commas in the certificate.

Type: DistinguishedName object

Required: No

DnsName

Represents `GeneralName` as a DNS name.

Type: String

Required: No

IpAddress

Represents `GeneralName` as an IPv4 or IPv6 address.

Type: String

Required: No

OtherName

Represents `GeneralName` using an `OtherName` object.

Type: OtherName object

Required: No

RegisteredId

Represents `GeneralName` as an object identifier (OID).

Type: String

Required: No

Rfc822Name

Represents `GeneralName` as an RFC 822 email address.

Type: String

Required: No

UniformResourceIdentifier

Represents `GeneralName` as a URI.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

HttpRedirect

Contains information for HTTP-based domain validation of certificates requested through Amazon CloudFront and issued by ACM. This field exists only when the certificate type is `AMAZON_ISSUED` and the validation method is `HTTP`.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

RedirectFrom

The URL including the domain to be validated. The certificate authority sends `GET` requests here during validation.

Type: String

Required: No

RedirectTo

The URL hosting the validation token. `RedirectFrom` must return this content or redirect here.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KeyUsage

The Key Usage X.509 v3 extension defines the purpose of the public key contained in the certificate.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

Name

A string value that contains a Key Usage extension name.

Type: String

Valid Values: `DIGITAL_SIGNATURE | NON_REPUDIATION | KEY_ENCIPHERMENT | DATA_ENCIPHERMENT | KEY_AGREEMENT | CERTIFICATE_SIGNING | CRL_SIGNING | ENCIPHER_ONLY | DECIPHER_ONLY | ANY | CUSTOM`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OtherName

Defines a custom ASN.1 X.400 `GeneralName` using an object identifier (OID) and value. For more information, see NIST's definition of Object Identifier (OID).

Contents

> **Note**
>
> In the following list, the required parameters are described first.

ObjectIdentifier

Specifies an OID.

Type: String

Required: No

Value

Specifies an OID value.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RenewalSummary

Contains information about the status of ACM's managed renewal for the certificate. This structure exists only when the certificate type is `AMAZON_ISSUED`.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

DomainValidationOptions

Contains information about the validation of each domain name in the certificate, as it pertains to ACM's managed renewal. This is different from the initial validation that occurs as a result of the RequestCertificate request. This field exists only when the certificate type is `AMAZON_ISSUED`.

Type: Array of DomainValidation objects

Array Members: Minimum number of 1 item. Maximum number of 1000 items.

Required: Yes

RenewalStatus

The status of ACM's managed renewal of the certificate.

Type: String

Valid Values: `PENDING_AUTO_RENEWAL | PENDING_VALIDATION | SUCCESS | FAILED`

Required: Yes

UpdatedAt

The time at which the renewal summary was last updated.

Type: Timestamp

Required: Yes

RenewalStatusReason

The reason that a renewal request was unsuccessful.

Type: String

Valid Values: `NO_AVAILABLE_CONTACTS | ADDITIONAL_VERIFICATION_REQUIRED | DOMAIN_NOT_ALLOWED | INVALID_PUBLIC_DOMAIN | DOMAIN_VALIDATION_DENIED | CAA_ERROR | PCA_LIMIT_EXCEEDED | PCA_INVALID_ARN | PCA_INVALID_STATE | PCA_REQUEST_FAILED | PCA_NAME_CONSTRAINTS_VALIDATION | PCA_RESOURCE_NOT_FOUND | PCA_INVALID_ARGS | PCA_INVALID_DURATION | PCA_ACCESS_DENIED | SLR_NOT_FOUND | OTHER`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ResourceRecord

Contains a DNS record value that you can use to validate ownership or control of a domain. This is used by the DescribeCertificate action.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

Name

The name of the DNS record to create in your domain. This is supplied by ACM.

Type: String

Required: Yes

Type

The type of DNS record. Currently this can be CNAME.

Type: String

Valid Values: CNAME

Required: Yes

Value

The value of the CNAME record to add to your DNS database. This is supplied by ACM.

Type: String

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SubjectAlternativeNameFilter

Filters certificates by subject alternative name attributes.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

> **Important**
>
> This data type is a UNION, so only one of the following members can be specified when used or returned.

DnsName

Filter by DNS name in subject alternative names.

Type: DnsNameFilter object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SubjectFilter

Filters certificates by subject attributes.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

> **Important**
>
> This data type is a UNION, so only one of the following members can be specified when used or returned.

CommonName

Filter by common name in the subject.

Type: CommonNameFilter object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Tag

A key-value pair that identifies or specifies metadata about an ACM resource.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

Key

The key of the tag.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\p{L}\p{Z}\p{N}_.:\/=+\-@]*`

Required: Yes

Value

The value of the tag.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[\p{L}\p{Z}\p{N}_.:\/=+\-@]*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

ThrottlingReason

A description of why a request was throttled.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

reason

A description of why a request was throttled.

Type: String

Required: No

resource

The resource that causes the request to be throttled.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TimestampRange

Specifies a time range for filtering certificates.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

End

The end of the time range. This value is inclusive.

Type: Timestamp

Required: No

Start

The start of the time range. This value is inclusive.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

X509AttributeFilter

Filters certificates by X.509 attributes.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

> **Important**
>
> This data type is a UNION, so only one of the following members can be specified when used or returned.

ExtendedKeyUsage

Filter by extended key usage.

Type: String

Valid Values: `TLS_WEB_SERVER_AUTHENTICATION | TLS_WEB_CLIENT_AUTHENTICATION | CODE_SIGNING | EMAIL_PROTECTION | TIME_STAMPING | OCSP_SIGNING | IPSEC_END_SYSTEM | IPSEC_TUNNEL | IPSEC_USER | ANY | NONE | CUSTOM`

Required: No

KeyAlgorithm

Filter by key algorithm.

Type: String

Valid Values: `RSA_1024 | RSA_2048 | RSA_3072 | RSA_4096 | EC_prime256v1 | EC_secp384r1 | EC_secp521r1`

Required: No

KeyUsage

Filter by key usage.

Type: String

Valid Values: `DIGITAL_SIGNATURE | NON_REPUDIATION | KEY_ENCIPHERMENT | DATA_ENCIPHERMENT | KEY_AGREEMENT | CERTIFICATE_SIGNING | CRL_SIGNING | ENCIPHER_ONLY | DECIPHER_ONLY | ANY | CUSTOM`

Required: No

NotAfter

Filter by certificate expiration date. The start date is inclusive.

Type: TimestampRange object

Required: No

NotBefore

Filter by certificate validity start date. The start date is inclusive.

Type: TimestampRange object

Required: No

SerialNumber

Filter by serial number.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 59.

Pattern: `[0-9a-f]{2}(:[0-9a-f]{2}){1,19}`

Required: No

Subject

Filter by certificate subject.

Type: SubjectFilter object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

SubjectAlternativeName

Filter by subject alternative names.

Type: SubjectAlternativeNameFilter object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

X509Attributes

Contains X.509 certificate attributes extracted from the certificate.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

ExtendedKeyUsages

Contains a list of Extended Key Usage X.509 v3 extension objects. Each object specifies a purpose for which the certificate public key can be used and consists of a name and an object identifier (OID).

Type: Array of strings

Valid Values: `TLS_WEB_SERVER_AUTHENTICATION | TLS_WEB_CLIENT_AUTHENTICATION | CODE_SIGNING | EMAIL_PROTECTION | TIME_STAMPING | OCSP_SIGNING | IPSEC_END_SYSTEM | IPSEC_TUNNEL | IPSEC_USER | ANY | NONE | CUSTOM`

Required: No

Issuer

The distinguished name of the certificate issuer.

Type: DistinguishedName object

Required: No

KeyAlgorithm

The algorithm that was used to generate the public-private key pair.

Type: String

Valid Values: `RSA_1024 | RSA_2048 | RSA_3072 | RSA_4096 | EC_prime256v1 | EC_secp384r1 | EC_secp521r1`

Required: No

KeyUsages

A list of Key Usage X.509 v3 extension objects. Each object is a string value that identifies the purpose of the public key contained in the certificate. Possible extension values include DIGITAL_SIGNATURE, KEY_ENCHIPHERMENT, NON_REPUDIATION, and more.

Type: Array of strings

Valid Values: `DIGITAL_SIGNATURE | NON_REPUDIATION | KEY_ENCIPHERMENT | DATA_ENCIPHERMENT | KEY_AGREEMENT | CERTIFICATE_SIGNING | CRL_SIGNING | ENCIPHER_ONLY | DECIPHER_ONLY | ANY | CUSTOM`

Required: No

NotAfter

The time after which the certificate is not valid.

Type: Timestamp

Required: No

NotBefore

The time before which the certificate is not valid.

Type: Timestamp

Required: No

SerialNumber

The serial number assigned by the certificate authority.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 59.

Pattern: `[0-9a-f]{2}(:[0-9a-f]{2}){1,19}`

Required: No

Subject

The distinguished name of the certificate subject.

Type: DistinguishedName object

Required: No

SubjectAlternativeNames

One or more domain names (subject alternative names) included in the certificate. This list contains the domain names that are bound to the public key that is contained in the certificate. The subject alternative names include the canonical domain name (CN) of the certificate and additional domain names that can be used to connect to the website.

Type: Array of GeneralName objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signing AWS API requests in the *IAM User Guide*.

X-Amz-Algorithm

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: *access_key*/*YYYYMMDD*/*region*/*service*/aws4_request.

For more information, see Create a signed AWS API request in the *IAM User Guide*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: `20120325T120000Z`.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Elements of an AWS API request signature in the *IAM User Guide*.

Type: string

Required: Conditional

X-Amz-Security-Token

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS STS, see AWS services that work with IAM in the *IAM User Guide*.

Condition: If you're using temporary security credentials from AWS STS, you must include the security token.

Type: string

Required: Conditional

X-Amz-Signature

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Create a signed AWS API request in the *IAM User Guide*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

Common Error Types

This section lists common error types that this AWS service may return. Not all services return all error types listed here. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You don't have permission to perform this action. Verify that your IAM policy includes the required permissions.

HTTP Status Code: 403

ExpiredTokenException

The security token included in the request has expired. Request a new security token and try again.

HTTP Status Code: 403

IncompleteSignature

The request signature doesn't conform to AWS standards. Verify that you're using valid AWS credentials and that your request is properly formatted. If you're using an SDK, ensure it's up to date.

HTTP Status Code: 403

InternalFailure

The request can't be processed right now because of an internal server issue. Try again later. If the problem persists, contact AWS Support.

HTTP Status Code: 500

MalformedHttpRequestException

The request body can't be processed. This typically happens when the request body can't be decompressed using the specified content encoding algorithm. Verify that the content encoding header matches the compression format used.

HTTP Status Code: 400

NotAuthorized

You don't have permissions to perform this action. Verify that your IAM policy includes the required permissions.

HTTP Status Code: 401

OptInRequired

Your AWS account needs a subscription for this service. Verify that you've enabled the service in your account.

HTTP Status Code: 403

RequestAbortedException

The request was aborted before a response could be returned. This typically happens when the client closes the connection.

HTTP Status Code: 400

RequestEntityTooLargeException

The request entity is too large. Reduce the size of the request body and try again.

HTTP Status Code: 413

RequestTimeoutException

The request timed out. The server didn't receive the complete request within the expected time frame. Try again.

HTTP Status Code: 408

ServiceUnavailable

The service is temporarily unavailable. Try again later.

HTTP Status Code: 503

ThrottlingException

Your request rate is too high. The AWS SDKs automatically retry requests that receive this exception. Reduce the frequency of requests.

HTTP Status Code: 400

UnknownOperationException

The action or operation isn't recognized. Verify that the action name is spelled correctly and that it's supported by the API version you're using.

HTTP Status Code: 404

UnrecognizedClientException

The X.509 certificate or AWS access key ID you provided doesn't exist in our records. Verify that you're using valid credentials and that they haven't expired.

HTTP Status Code: 403

ValidationError

The input doesn't meet the required format or constraints. Check that all required parameters are included and that values are valid.

HTTP Status Code: 400