



API Reference

Amazon Cognito User Pools



API Version 2016-04-18

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

Amazon Cognito User Pools: API Reference

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

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

Table of Contents

Welcome	1
Actions	3
AddCustomAttributes	8
Request Syntax	8
Request Parameters	9
Response Elements	10
Errors	10
Examples	12
See Also	13
AddUserPoolClientSecret	14
Request Syntax	14
Request Parameters	14
Response Syntax	15
Response Elements	15
Errors	15
See Also	17
AdminAddUserToGroup	18
Request Syntax	18
Request Parameters	18
Response Elements	19
Errors	19
Examples	21
See Also	22
AdminConfirmSignUp	23
Request Syntax	23
Request Parameters	23
Response Elements	25
Errors	25
Examples	28
See Also	29
AdminCreateUser	30
Request Syntax	31
Request Parameters	31
Response Syntax	36

Response Elements	37
Errors	37
Examples	41
See Also	43
AdminDeleteUser	44
Request Syntax	44
Request Parameters	44
Response Elements	45
Errors	45
Examples	46
See Also	47
AdminDeleteUserAttributes	49
Request Syntax	49
Request Parameters	49
Response Elements	50
Errors	50
Examples	52
See Also	53
AdminDisableProviderForUser	54
Request Syntax	55
Request Parameters	55
Response Elements	55
Errors	55
See Also	57
AdminDisableUser	59
Request Syntax	59
Request Parameters	59
Response Elements	60
Errors	60
Examples	62
See Also	62
AdminEnableUser	64
Request Syntax	64
Request Parameters	64
Response Elements	65
Errors	65

Examples	66
See Also	67
AdminForgetDevice	69
Request Syntax	69
Request Parameters	69
Response Elements	70
Errors	70
Examples	72
See Also	73
AdminGetDevice	74
Request Syntax	74
Request Parameters	74
Response Syntax	75
Response Elements	76
Errors	76
Examples	77
See Also	79
AdminGetUser	81
Request Syntax	81
Request Parameters	81
Response Syntax	82
Response Elements	83
Errors	85
Examples	86
See Also	88
AdminInitiateAuth	90
Request Syntax	90
Request Parameters	91
Response Syntax	96
Response Elements	97
Errors	100
Examples	104
See Also	106
AdminLinkProviderForUser	107
Request Syntax	107
Request Parameters	108

Response Elements	109
Errors	110
Examples	112
See Also	118
AdminListDevices	119
Request Syntax	119
Request Parameters	119
Response Syntax	121
Response Elements	121
Errors	122
Examples	123
See Also	126
AdminListGroupsWithUser	127
Request Syntax	127
Request Parameters	127
Response Syntax	129
Response Elements	129
Errors	130
Examples	131
See Also	132
AdminListUserAuthEvents	134
Request Syntax	134
Request Parameters	134
Response Syntax	136
Response Elements	136
Errors	137
Examples	139
See Also	141
AdminRemoveUserFromGroup	142
Request Syntax	142
Request Parameters	142
Response Elements	143
Errors	143
Examples	145
See Also	146
AdminResetUserPassword	147

Request Syntax	148
Request Parameters	148
Response Elements	150
Errors	150
Examples	153
See Also	154
AdminRespondToAuthChallenge	155
Request Syntax	156
Request Parameters	156
Response Syntax	164
Response Elements	165
Errors	168
Examples	173
See Also	174
AdminSetUserMFAPreference	176
Request Syntax	176
Request Parameters	177
Response Elements	178
Errors	178
Examples	180
See Also	181
AdminSetUserPassword	183
Request Syntax	184
Request Parameters	184
Response Elements	185
Errors	185
Examples	187
See Also	188
AdminSetUserSettings	189
Request Syntax	189
Request Parameters	189
Response Elements	190
Errors	190
See Also	192
AdminUpdateAuthEventFeedback	193
Request Syntax	193

Request Parameters	193
Response Elements	195
Errors	195
See Also	197
AdminUpdateDeviceStatus	198
Request Syntax	198
Request Parameters	198
Response Elements	200
Errors	200
Examples	201
See Also	202
AdminUpdateUserAttributes	204
Request Syntax	205
Request Parameters	205
Response Elements	207
Errors	207
Examples	211
See Also	212
AdminUserGlobalSignOut	213
Request Syntax	213
Request Parameters	214
Response Elements	214
Errors	215
Examples	216
See Also	217
AssociateSoftwareToken	218
Request Syntax	218
Request Parameters	219
Response Syntax	219
Response Elements	219
Errors	220
Examples	222
See Also	223
ChangePassword	224
Request Syntax	224
Request Parameters	224

Response Elements	225
Errors	225
Examples	228
See Also	229
CompleteWebAuthnRegistration	230
Request Syntax	230
Request Parameters	230
Response Elements	231
Errors	231
Examples	233
See Also	234
ConfirmDevice	235
Request Syntax	235
Request Parameters	235
Response Syntax	236
Response Elements	237
Errors	237
Examples	240
See Also	241
ConfirmForgotPassword	243
Request Syntax	243
Request Parameters	243
Response Elements	246
Errors	247
Examples	250
See Also	251
ConfirmSignUp	252
Request Syntax	252
Request Parameters	253
Response Syntax	256
Response Elements	256
Errors	257
Examples	261
See Also	262
CreateGroup	263
Request Syntax	263

Request Parameters	263
Response Syntax	265
Response Elements	265
Errors	266
Examples	267
See Also	268
CreateIdentityProvider	270
Request Syntax	270
Request Parameters	270
Response Syntax	275
Response Elements	275
Errors	276
Examples	277
See Also	282
CreateManagedLoginBranding	283
Request Syntax	283
Request Parameters	284
Response Syntax	285
Response Elements	286
Errors	286
Examples	288
See Also	310
CreateResourceServer	312
Request Syntax	312
Request Parameters	312
Response Syntax	314
Response Elements	314
Errors	314
Examples	316
See Also	317
CreateTerms	319
Request Syntax	319
Request Parameters	320
Response Syntax	321
Response Elements	322
Errors	322

Examples	324
See Also	325
CreateUserImportJob	327
Request Syntax	327
Request Parameters	327
Response Syntax	328
Response Elements	329
Errors	329
Examples	331
See Also	332
CreateUserPool	333
Request Syntax	334
Request Parameters	337
Response Syntax	344
Response Elements	347
Errors	347
Examples	350
See Also	362
CreateUserPoolClient	363
Request Syntax	363
Request Parameters	364
Response Syntax	376
Response Elements	377
Errors	377
Examples	379
See Also	382
CreateUserPoolDomain	384
Request Syntax	384
Request Parameters	384
Response Syntax	386
Response Elements	386
Errors	387
Examples	388
See Also	389
DeleteGroup	391
Request Syntax	391

Request Parameters	391
Response Elements	392
Errors	392
Examples	393
See Also	394
DeleteIdentityProvider	395
Request Syntax	395
Request Parameters	395
Response Elements	396
Errors	396
Examples	398
See Also	398
DeleteManagedLoginBranding	399
Request Syntax	399
Request Parameters	399
Response Elements	400
Errors	400
Examples	402
See Also	402
DeleteResourceServer	404
Request Syntax	404
Request Parameters	404
Response Elements	405
Errors	405
Examples	406
See Also	407
DeleteTerms	408
Request Syntax	408
Request Parameters	408
Response Elements	409
Errors	409
Examples	410
See Also	411
DeleteUser	412
Request Syntax	412
Request Parameters	412

Response Elements	413
Errors	413
Examples	415
See Also	415
DeleteUserAttributes	417
Request Syntax	417
Request Parameters	417
Response Elements	418
Errors	418
Examples	420
See Also	421
DeleteUserPool	422
Request Syntax	422
Request Parameters	422
Response Elements	422
Errors	423
Examples	424
See Also	425
DeleteUserPoolClient	427
Request Syntax	427
Request Parameters	427
Response Elements	428
Errors	428
Examples	429
See Also	430
DeleteUserPoolClientSecret	431
Request Syntax	431
Request Parameters	431
Response Elements	432
Errors	432
See Also	433
DeleteUserPoolDomain	434
Request Syntax	434
Request Parameters	434
Response Elements	435
Errors	435

Examples	436
See Also	437
DeleteWebAuthnCredential	438
Request Syntax	438
Request Parameters	438
Response Elements	439
Errors	439
Examples	441
See Also	442
DescribeIdentityProvider	443
Request Syntax	443
Request Parameters	443
Response Syntax	444
Response Elements	444
Errors	444
Examples	446
See Also	447
DescribeManagedLoginBranding	448
Request Syntax	448
Request Parameters	448
Response Syntax	449
Response Elements	449
Errors	450
Examples	451
See Also	462
DescribeManagedLoginBrandingByClient	464
Request Syntax	464
Request Parameters	464
Response Syntax	465
Response Elements	465
Errors	466
Examples	467
See Also	478
DescribeResourceServer	480
Request Syntax	480
Request Parameters	480

Response Syntax	481
Response Elements	481
Errors	481
Examples	483
See Also	484
DescribeRiskConfiguration	485
Request Syntax	485
Request Parameters	485
Response Syntax	486
Response Elements	487
Errors	487
Examples	489
See Also	491
DescribeTerms	493
Request Syntax	493
Request Parameters	493
Response Syntax	494
Response Elements	494
Errors	495
Examples	496
See Also	497
DescribeUserImportJob	498
Request Syntax	498
Request Parameters	498
Response Syntax	499
Response Elements	499
Errors	499
Examples	501
See Also	502
DescribeUserPool	503
Request Syntax	503
Request Parameters	503
Response Syntax	504
Response Elements	507
Errors	507
Examples	509

See Also	517
DescribeUserPoolClient	519
Request Syntax	519
Request Parameters	519
Response Syntax	520
Response Elements	521
Errors	521
Examples	523
See Also	525
DescribeUserPoolDomain	526
Request Syntax	526
Request Parameters	526
Response Syntax	527
Response Elements	527
Errors	527
Examples	528
See Also	529
ForgetDevice	531
Request Syntax	531
Request Parameters	531
Response Elements	532
Errors	532
Examples	534
See Also	535
ForgotPassword	536
Request Syntax	537
Request Parameters	537
Response Syntax	540
Response Elements	540
Errors	540
Examples	544
See Also	545
GetCSVHeader	546
Request Syntax	546
Request Parameters	546
Response Syntax	547

Response Elements	547
Errors	547
Examples	549
See Also	550
GetDevice	552
Request Syntax	552
Request Parameters	552
Response Syntax	553
Response Elements	553
Errors	554
Examples	556
See Also	557
GetGroup	559
Request Syntax	559
Request Parameters	559
Response Syntax	560
Response Elements	560
Errors	561
Examples	562
See Also	563
GetIdentityProviderByIdentifier	564
Request Syntax	564
Request Parameters	564
Response Syntax	565
Response Elements	565
Errors	565
Examples	567
See Also	568
GetLogDeliveryConfiguration	570
Request Syntax	570
Request Parameters	570
Response Syntax	571
Response Elements	571
Errors	571
Examples	573
See Also	574

GetSigningCertificate	575
Request Syntax	575
Request Parameters	575
Response Syntax	576
Response Elements	576
Errors	576
Examples	577
See Also	578
GetTokensFromRefreshToken	579
Request Syntax	579
Request Parameters	579
Response Syntax	581
Response Elements	582
Errors	582
See Also	585
GetUICustomization	586
Request Syntax	586
Request Parameters	586
Response Syntax	587
Response Elements	587
Errors	587
Examples	589
See Also	590
GetUser	591
Request Syntax	591
Request Parameters	591
Response Syntax	592
Response Elements	592
Errors	593
Examples	595
See Also	597
GetUserAttributeVerificationCode	599
Request Syntax	599
Request Parameters	600
Response Syntax	601
Response Elements	602

Errors	602
Examples	606
See Also	607
GetUserAuthFactors	608
Request Syntax	608
Request Parameters	608
Response Syntax	609
Response Elements	609
Errors	610
Examples	612
See Also	613
GetUserPoolMfaConfig	615
Request Syntax	615
Request Parameters	615
Response Syntax	616
Response Elements	616
Errors	618
Examples	619
See Also	620
GlobalSignOut	622
Request Syntax	622
Request Parameters	623
Response Elements	623
Errors	623
Examples	625
See Also	626
InitiateAuth	627
Request Syntax	627
Request Parameters	628
Response Syntax	633
Response Elements	633
Errors	637
Examples	641
See Also	645
ListDevices	647
Request Syntax	647

Request Parameters	647
Response Syntax	648
Response Elements	649
Errors	649
Examples	652
See Also	653
ListGroups	655
Request Syntax	655
Request Parameters	655
Response Syntax	656
Response Elements	657
Errors	657
Examples	659
See Also	660
ListIdentityProviders	661
Request Syntax	661
Request Parameters	661
Response Syntax	662
Response Elements	663
Errors	663
Examples	664
See Also	666
ListResourceServers	667
Request Syntax	667
Request Parameters	667
Response Syntax	668
Response Elements	669
Errors	669
Examples	671
See Also	672
ListTagsForResource	673
Request Syntax	673
Request Parameters	673
Response Syntax	673
Response Elements	673
Errors	674

Examples	675
See Also	676
ListTerms	677
Request Syntax	677
Request Parameters	677
Response Syntax	678
Response Elements	679
Errors	679
Examples	680
See Also	682
ListUserImportJobs	683
Request Syntax	683
Request Parameters	683
Response Syntax	684
Response Elements	685
Errors	685
Examples	687
See Also	689
ListUserPoolClients	690
Request Syntax	690
Request Parameters	690
Response Syntax	691
Response Elements	692
Errors	692
Examples	693
See Also	695
ListUserPoolClientSecrets	696
Request Syntax	696
Request Parameters	696
Response Syntax	697
Response Elements	697
Errors	697
See Also	698
ListUserPools	700
Request Syntax	700
Request Parameters	700

Response Syntax	701
Response Elements	702
Errors	703
Examples	704
See Also	705
ListUsers	707
Request Syntax	707
Request Parameters	707
Response Syntax	710
Response Elements	711
Errors	712
Examples	713
See Also	715
ListUsersInGroup	716
Request Syntax	716
Request Parameters	716
Response Syntax	718
Response Elements	718
Errors	719
Examples	720
See Also	723
ListWebAuthnCredentials	725
Request Syntax	725
Request Parameters	725
Response Syntax	726
Response Elements	727
Errors	727
Examples	729
See Also	730
ResendConfirmationCode	731
Request Syntax	731
Request Parameters	732
Response Syntax	734
Response Elements	735
Errors	735
Examples	739

See Also	740
RespondToAuthChallenge	741
Request Syntax	742
Request Parameters	742
Response Syntax	750
Response Elements	751
Errors	754
Examples	759
See Also	760
RevokeToken	761
Request Syntax	761
Request Parameters	761
Response Elements	762
Errors	762
Examples	764
See Also	764
SetLogDeliveryConfiguration	766
Request Syntax	766
Request Parameters	766
Response Syntax	767
Response Elements	767
Errors	768
Examples	769
See Also	772
SetRiskConfiguration	774
Request Syntax	774
Request Parameters	775
Response Syntax	777
Response Elements	778
Errors	778
Examples	780
See Also	787
SetUICustomization	788
Request Syntax	788
Request Parameters	788
Response Syntax	790

Response Elements	790
Errors	790
Examples	792
See Also	794
SetUserMFAPreference	795
Request Syntax	795
Request Parameters	796
Response Elements	797
Errors	797
Examples	799
See Also	800
SetUserPoolMfaConfig	802
Request Syntax	802
Request Parameters	803
Response Syntax	804
Response Elements	805
Errors	806
Examples	808
See Also	810
SetUserSettings	812
Request Syntax	812
Request Parameters	812
Response Elements	813
Errors	813
See Also	815
SignUp	816
Request Syntax	817
Request Parameters	817
Response Syntax	821
Response Elements	821
Errors	822
Examples	826
See Also	827
StartUserImportJob	829
Request Syntax	829
Request Parameters	829

Response Syntax	830
Response Elements	830
Errors	830
Examples	832
See Also	833
StartWebAuthnRegistration	835
Request Syntax	835
Request Parameters	835
Response Syntax	835
Response Elements	836
Errors	836
Examples	838
See Also	839
StopUserImportJob	841
Request Syntax	841
Request Parameters	841
Response Syntax	842
Response Elements	842
Errors	842
Examples	844
See Also	845
TagResource	847
Request Syntax	847
Request Parameters	847
Response Elements	848
Errors	848
Examples	849
See Also	850
UntagResource	852
Request Syntax	852
Request Parameters	852
Response Elements	852
Errors	853
Examples	854
See Also	855
UpdateAuthEventFeedback	856

Request Syntax	856
Request Parameters	856
Response Elements	858
Errors	858
See Also	860
UpdateDeviceStatus	861
Request Syntax	861
Request Parameters	861
Response Elements	862
Errors	862
Examples	865
See Also	865
UpdateGroup	867
Request Syntax	867
Request Parameters	867
Response Syntax	869
Response Elements	869
Errors	870
Examples	871
See Also	872
UpdateIdentityProvider	873
Request Syntax	873
Request Parameters	873
Response Syntax	878
Response Elements	878
Errors	878
Examples	880
See Also	882
UpdateManagedLoginBranding	883
Request Syntax	883
Request Parameters	884
Response Syntax	885
Response Elements	886
Errors	886
Examples	888
See Also	910

UpdateResourceServer	911
Request Syntax	911
Request Parameters	911
Response Syntax	913
Response Elements	913
Errors	913
Examples	915
See Also	916
UpdateTerms	917
Request Syntax	917
Request Parameters	918
Response Syntax	919
Response Elements	920
Errors	920
Examples	922
See Also	923
UpdateUserAttributes	925
Request Syntax	926
Request Parameters	926
Response Syntax	928
Response Elements	928
Errors	928
Examples	933
See Also	934
UpdateUserPool	936
Request Syntax	937
Request Parameters	939
Response Elements	945
Errors	946
Examples	948
See Also	951
UpdateUserPoolClient	952
Request Syntax	952
Request Parameters	953
Response Syntax	964
Response Elements	965

Errors	965
Examples	967
See Also	973
UpdateUserPoolDomain	974
Request Syntax	974
Request Parameters	975
Response Syntax	976
Response Elements	976
Errors	977
Examples	979
See Also	980
VerifySoftwareToken	981
Request Syntax	981
Request Parameters	981
Response Syntax	982
Response Elements	982
Errors	983
Examples	986
See Also	987
VerifyUserAttribute	988
Request Syntax	988
Request Parameters	988
Response Elements	989
Errors	989
Examples	993
See Also	993
Data Types	995
AccountRecoverySettingType	999
Contents	999
See Also	999
AccountTakeoverActionsType	1000
Contents	1000
See Also	1000
AccountTakeoverActionType	1002
Contents	1002
See Also	1003

AccountTakeoverRiskConfigurationType	1004
Contents	1004
See Also	1004
AdminCreateUserConfigType	1005
Contents	1005
See Also	1006
AdvancedSecurityAdditionalFlowsType	1007
Contents	1007
See Also	1007
AnalyticsConfigurationType	1008
Contents	1008
See Also	1009
AnalyticsMetadataType	1011
Contents	1011
See Also	1011
AssetType	1012
Contents	1012
See Also	1013
AttributeType	1014
Contents	1014
See Also	1014
AuthenticationResultType	1016
Contents	1016
See Also	1017
AuthEventType	1018
Contents	1018
See Also	1020
ChallengeResponseType	1021
Contents	1024
See Also	1024
ClientSecretDescriptorType	1026
Contents	1026
See Also	1026
ClientSecretListDescriptorType	1028
Contents	1028
See Also	1028

CloudWatchLogsConfigurationType	1029
Contents	1029
See Also	1029
CodeDeliveryDetailsType	1030
Contents	1030
See Also	1031
CompromisedCredentialsActionsType	1032
Contents	1032
See Also	1032
CompromisedCredentialsRiskConfigurationType	1033
Contents	1033
See Also	1033
ContextDataType	1034
Contents	1034
See Also	1035
CustomDomainConfigType	1036
Contents	1036
See Also	1036
CustomEmailLambdaVersionConfigType	1037
Contents	1037
See Also	1037
CustomSMSLambdaVersionConfigType	1039
Contents	1039
See Also	1039
DeviceConfigurationType	1041
Contents	1041
See Also	1042
DeviceSecretVerifierConfigType	1043
Contents	1043
See Also	1043
DeviceType	1044
Contents	1044
See Also	1045
DomainDescriptionType	1046
Contents	1046
See Also	1048

EmailConfigurationType	1049
Contents	1049
See Also	1052
EmailMfaConfigType	1053
Contents	1053
See Also	1053
EmailMfaSettingsType	1055
Contents	1055
See Also	1055
EventContextDataType	1056
Contents	1056
See Also	1057
EventFeedbackType	1058
Contents	1058
See Also	1059
EventRiskType	1060
Contents	1060
See Also	1060
FirehoseConfigurationType	1062
Contents	1062
See Also	1062
GroupType	1063
Contents	1063
See Also	1065
HTTPHeader	1066
Contents	1066
See Also	1066
IdentityProviderType	1067
Contents	1067
See Also	1072
InboundFederationLambdaType	1073
Contents	1073
See Also	1073
LambdaConfigType	1075
Contents	1075
See Also	1079

LogConfigurationType	1080
Contents	1080
See Also	1081
LogDeliveryConfigurationType	1082
Contents	1082
See Also	1082
ManagedLoginBrandingType	1083
Contents	1083
See Also	1085
MessageTemplateType	1086
Contents	1086
See Also	1087
MFAOptionType	1088
Contents	1088
See Also	1088
NewDeviceMetadataType	1090
Contents	1090
See Also	1090
NotifyConfigurationType	1092
Contents	1092
See Also	1093
NotifyEmailType	1094
Contents	1094
See Also	1095
NumberAttributeConstraintsType	1096
Contents	1096
See Also	1096
PasswordPolicyType	1098
Contents	1098
See Also	1100
PreTokenGenerationVersionConfigType	1101
Contents	1101
See Also	1101
ProviderDescription	1103
Contents	1103
See Also	1104

ProviderUserIdentifierType	1105
Contents	1105
See Also	1106
RecoveryOptionType	1107
Contents	1107
See Also	1107
RefreshTokenRotationType	1109
Contents	1109
See Also	1109
ResourceServerScopeType	1111
Contents	1111
See Also	1111
ResourceServerType	1113
Contents	1113
See Also	1114
RiskConfigurationType	1115
Contents	1115
See Also	1116
RiskExceptionConfigurationType	1117
Contents	1117
See Also	1117
S3ConfigurationType	1119
Contents	1119
See Also	1119
SchemaAttributeType	1120
Contents	1120
See Also	1122
SignInPolicyType	1123
Contents	1123
See Also	1123
SmsConfigurationType	1124
Contents	1124
See Also	1125
SmsMfaConfigType	1126
Contents	1126
See Also	1126

SMSMfaSettingsType	1128
Contents	1128
See Also	1128
SoftwareTokenMfaConfigType	1129
Contents	1129
See Also	1129
SoftwareTokenMfaSettingsType	1130
Contents	1130
See Also	1130
StringAttributeConstraintsType	1131
Contents	1131
See Also	1131
TermsDescriptionType	1133
Contents	1133
See Also	1134
TermsType	1135
Contents	1135
See Also	1137
TokenValidityUnitsType	1138
Contents	1138
See Also	1139
UICustomizationType	1140
Contents	1140
See Also	1141
UserAttributeUpdateSettingsType	1143
Contents	1143
See Also	1143
UserContextDataType	1145
Contents	1145
See Also	1145
UserImportJobType	1147
Contents	1147
See Also	1150
UsernameConfigurationType	1151
Contents	1151
See Also	1151

UserPoolAddOnsType	1153
Contents	1153
See Also	1153
UserPoolClientDescription	1155
Contents	1155
See Also	1156
UserPoolClientType	1157
Contents	1157
See Also	1168
UserPoolDescriptionType	1170
Contents	1170
See Also	1171
UserPoolPolicyType	1172
Contents	1172
See Also	1172
UserPoolType	1173
Contents	1173
See Also	1182
UserType	1183
Contents	1183
See Also	1184
VerificationMessageTemplateType	1186
Contents	1186
See Also	1188
WebAuthnConfigurationType	1189
Contents	1189
See Also	1190
WebAuthnCredentialDescription	1191
Contents	1191
See Also	1192
WebAuthnMfaSettingsType	1193
Contents	1193
See Also	1193
Common Parameters	1194
Common Error Types	1197

Welcome

With the Amazon Cognito user pools API, you can configure user pools and authenticate users. To authenticate users from third-party identity providers (IdPs) in this API, you can [link IdP users to native user profiles](#). Learn more about the authentication and authorization of federated users at [Adding user pool sign-in through a third party](#) and in the [User pool federation endpoints and managed login reference](#).

This API reference provides detailed information about API operations and object types in Amazon Cognito.

Along with resource management operations, the Amazon Cognito user pools API includes classes of operations and authorization models for client-side and server-side authentication of users. You can interact with operations in the Amazon Cognito user pools API as any of the following subjects.

1. An administrator who wants to configure user pools, app clients, users, groups, or other user pool functions.
2. A server-side app, like a web application, that wants to use its AWS privileges to manage, authenticate, or authorize a user.
3. A client-side app, like a mobile app, that wants to make unauthenticated requests to manage, authenticate, or authorize a user.

For more information, see [Understanding API, OIDC, and managed login pages authentication](#) in the *Amazon Cognito Developer Guide*.

With your AWS SDK, you can build the logic to support operational flows in every use case for this API. You can also make direct REST API requests to [Amazon Cognito user pools service endpoints](#). The following links can get you started with the `CognitoIdentityProvider` client in supported AWS SDKs.

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)

- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
- [AWS SDK for Kotlin](#)

To get started with an AWS SDK, see [Tools to Build on AWS](#). For example actions and scenarios, see [Code examples for Amazon Cognito Identity Provider using AWS SDKs](#).

This document was last published on April 10, 2026.

Actions

The following actions are supported:

- [AddCustomAttributes](#)
- [AddUserPoolClientSecret](#)
- [AdminAddUserToGroup](#)
- [AdminConfirmSignUp](#)
- [AdminCreateUser](#)
- [AdminDeleteUser](#)
- [AdminDeleteUserAttributes](#)
- [AdminDisableProviderForUser](#)
- [AdminDisableUser](#)
- [AdminEnableUser](#)
- [AdminForgetDevice](#)
- [AdminGetDevice](#)
- [AdminGetUser](#)
- [AdminInitiateAuth](#)
- [AdminLinkProviderForUser](#)
- [AdminListDevices](#)
- [AdminListGroupsForUser](#)
- [AdminListUserAuthEvents](#)
- [AdminRemoveUserFromGroup](#)
- [AdminResetUserPassword](#)
- [AdminRespondToAuthChallenge](#)
- [AdminSetUserMFAPreference](#)
- [AdminSetUserPassword](#)
- [AdminSetUserSettings](#)
- [AdminUpdateAuthEventFeedback](#)
- [AdminUpdateDeviceStatus](#)
- [AdminUpdateUserAttributes](#)

- [AdminUserGlobalSignOut](#)
- [AssociateSoftwareToken](#)
- [ChangePassword](#)
- [CompleteWebAuthnRegistration](#)
- [ConfirmDevice](#)
- [ConfirmForgotPassword](#)
- [ConfirmSignUp](#)
- [CreateGroup](#)
- [CreateIdentityProvider](#)
- [CreateManagedLoginBranding](#)
- [CreateResourceServer](#)
- [CreateTerms](#)
- [CreateUserImportJob](#)
- [CreateUserPool](#)
- [CreateUserPoolClient](#)
- [CreateUserPoolDomain](#)
- [DeleteGroup](#)
- [DeleteIdentityProvider](#)
- [DeleteManagedLoginBranding](#)
- [DeleteResourceServer](#)
- [DeleteTerms](#)
- [DeleteUser](#)
- [DeleteUserAttributes](#)
- [DeleteUserPool](#)
- [DeleteUserPoolClient](#)
- [DeleteUserPoolClientSecret](#)
- [DeleteUserPoolDomain](#)
- [DeleteWebAuthnCredential](#)
- [DescribeIdentityProvider](#)
- [DescribeManagedLoginBranding](#)

- [DescribeManagedLoginBrandingByClient](#)
- [DescribeResourceServer](#)
- [DescribeRiskConfiguration](#)
- [DescribeTerms](#)
- [DescribeUserImportJob](#)
- [DescribeUserPool](#)
- [DescribeUserPoolClient](#)
- [DescribeUserPoolDomain](#)
- [ForgetDevice](#)
- [ForgotPassword](#)
- [GetCSVHeader](#)
- [GetDevice](#)
- [GetGroup](#)
- [GetIdentityProviderByIdentifier](#)
- [GetLogDeliveryConfiguration](#)
- [GetSigningCertificate](#)
- [GetTokensFromRefreshToken](#)
- [GetUICustomization](#)
- [GetUser](#)
- [GetUserAttributeVerificationCode](#)
- [GetUserAuthFactors](#)
- [GetUserPoolMfaConfig](#)
- [GlobalSignOut](#)
- [InitiateAuth](#)
- [ListDevices](#)
- [ListGroups](#)
- [ListIdentityProviders](#)
- [ListResourceServers](#)
- [ListTagsForResource](#)
- [ListTerms](#)

- [ListUserImportJobs](#)
- [ListUserPoolClients](#)
- [ListUserPoolClientSecrets](#)
- [ListUserPools](#)
- [ListUsers](#)
- [ListUsersInGroup](#)
- [ListWebAuthnCredentials](#)
- [ResendConfirmationCode](#)
- [RespondToAuthChallenge](#)
- [RevokeToken](#)
- [SetLogDeliveryConfiguration](#)
- [SetRiskConfiguration](#)
- [SetUICustomization](#)
- [SetUserMFAPreference](#)
- [SetUserPoolMfaConfig](#)
- [SetUserSettings](#)
- [SignUp](#)
- [StartUserImportJob](#)
- [StartWebAuthnRegistration](#)
- [StopUserImportJob](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateAuthEventFeedback](#)
- [UpdateDeviceStatus](#)
- [UpdateGroup](#)
- [UpdateIdentityProvider](#)
- [UpdateManagedLoginBranding](#)
- [UpdateResourceServer](#)
- [UpdateTerms](#)
- [UpdateUserAttributes](#)

- [UpdateUserPool](#)
- [UpdateUserPoolClient](#)
- [UpdateUserPoolDomain](#)
- [VerifySoftwareToken](#)
- [VerifyUserAttribute](#)

AddCustomAttributes

Adds additional user attributes to the user pool schema. Custom attributes can be mutable or immutable and have a `custom:` or `dev:` prefix. For more information, see [Custom attributes](#).

You can also create custom attributes in the [CreateUserPool](#) of `CreateUserPool` and `UpdateUserPool`. You can't delete custom attributes after you create them.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "CustomAttributes": [
    {
      "AttributeDataType": "string",
      "DeveloperOnlyAttribute": boolean,
      "Mutable": boolean,
      "Name": "string",
      "NumberAttributeConstraints": {
        "MaxValue": "string",
        "MinValue": "string"
      },
      "Required": boolean,
      "StringAttributeConstraints": {
        "MaxLength": "string",
        "MinLength": "string"
      }
    }
  ],
}
```

```
"UserPoolId": "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.

[CustomAttributes](#)

An array of custom attribute names and other properties. Sets the following characteristics:

AttributeDataType

The expected data type. Can be a string, a number, a date and time, or a boolean.

Mutable

If true, you can grant app clients write access to the attribute value. If false, the attribute value can only be set up on sign-up or administrator creation of users.

Name

The attribute name. For an attribute like `custom:myAttribute`, enter `myAttribute` for this field.

Required

When true, users who sign up or are created must set a value for the attribute.

NumberAttributeConstraints

The minimum and maximum length of accepted values for a `Number`-type attribute.

StringAttributeConstraints

The minimum and maximum length of accepted values for a `String`-type attribute.

DeveloperOnlyAttribute

This legacy option creates an attribute with a `dev :` prefix. You can only set the value of a developer-only attribute with administrative IAM credentials.

Type: Array of [SchemaAttributeType](#) objects

Array Members: Minimum number of 1 item. Maximum number of 25 items.

Required: Yes

UserPoolId

The ID of the user pool where you want to add custom attributes.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserImportInProgressException

This exception is thrown when you're trying to modify a user pool while a user import job is in progress for that pool.

message

The message returned when the user pool has an import job running.

HTTP Status Code: 400

Examples

Example

This example request adds the mutable custom attribute `custom:deliverables`, a string with a maximum length of 255 characters, to the user pool schema.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AddCustomAttributes
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "CustomAttributes": [
    {
      "AttributeDataType": "String",
      "DeveloperOnlyAttribute": false,
      "Mutable": true,
      "Name": "deliverables",
      "Required": false,
      "StringAttributeConstraints": {
        "MaxLength": "255",
        "MinLength": "1"
      }
    }
  ],
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
```

```
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{}
```

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](#)

AddUserPoolClientSecret

Creates a new client secret for an existing confidential user pool app client. Supports up to 2 active secrets per app client for zero-downtime credential rotation workflows.

Request Syntax

```
{  
  "ClientId": "string",  
  "ClientSecret": "string",  
  "UserPoolId": "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.

ClientId

The ID of the app client for which you want to create a new secret.

Type: String

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

Pattern: `[\w+]`+

Required: Yes

ClientSecret

The client secret value you want to use. If you don't provide this parameter, Amazon Cognito generates a secure secret for you.

Type: String

Length Constraints: Minimum length of 24. Maximum length of 64.

Pattern: `[\w+]`+

Required: No

UserPoolId

The ID of the user pool that contains the app client.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "ClientSecretDescriptor": {
    "ClientSecretCreateDate": number,
    "ClientSecretId": "string",
    "ClientSecretValue": "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.

ClientSecretDescriptor

The details of the newly created client secret, including its unique identifier and creation timestamp. The ClientSecretValue is only returned when Amazon Cognito generates the secret. For custom secrets that you provide, the ClientSecretValue is not included in the response.

Type: [ClientSecretDescriptorType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AccessDeniedException

This exception is thrown when you don't have sufficient permissions to perform the requested operation.

HTTP Status Code: 400

InternalServerErrorException

This exception is thrown when Amazon Cognito encounters an internal server error.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

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](#)

AdminAddUserToGroup

Adds a user to a group. A user who is in a group can present a preferred-role claim to an identity pool, and populates a `cognito:groups` claim to their access and identity tokens.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "GroupName": "string",  
  "Username": "string",  
  "UserPoolId": "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.

GroupName

The name of the group that you want to add your user to.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If `username` isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool that contains the group that you want to add the user to.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

This example request adds the user "testuser" to the group "testgroup."

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminAddUserToGroup
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "GroupName": "testgroup",
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
```

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](#)

AdminConfirmSignUp

Confirms user sign-up as an administrator.

Unlike [ConfirmSignUp](#), your IAM credentials authorize this operation to confirm user accounts. No confirmation code is required.

This request sets a user account active in a user pool that [requires confirmation of new user accounts](#) before they can sign in. You can configure your user pool to not send confirmation codes to new users and instead confirm them with this API operation on the back end.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

To configure your user pool to require administrative confirmation of users, set `AllowAdminCreateUserOnly` to `true` in a `CreateUserPool` or `UpdateUserPool` request.

Request Syntax

```
{
  "ClientMetadata": {
    "string" : "string"
  },
  "Username": "string",
  "UserPoolId": "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.

ClientMetadata

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If `username` isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to confirm a user's sign-up request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyFailedAttemptsException

This exception is thrown when the user has made too many failed attempts for a given action, such as sign-in.

message

The message returned when Amazon Cognito returns a TooManyFailedAttempts exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example operation confirms sign-up for the user "testuser." Note that because this is an administrative API operation, no confirmation code is required.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminConfirmSignUp
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser"
}
```

Sample Response

```
HTTP/1.1 200 OK
```

```
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
```

```
{}
```

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](#)

AdminCreateUser

Creates a new user in the specified user pool.

If `MessageAction` isn't set, the default is to send a welcome message via email or phone (SMS).

This message is based on a template that you configured in your call to create or update a user pool. This template includes your custom sign-up instructions and placeholders for user name and temporary password.

Alternatively, you can call `AdminCreateUser` with `SUPPRESS` for the `MessageAction` parameter, and Amazon Cognito won't send any email.

In either case, if the user has a password, they will be in the `FORCE_CHANGE_PASSWORD` state until they sign in and set their password. Your invitation message template must have the `{####}` password placeholder if your users have passwords. If your template doesn't have this placeholder, Amazon Cognito doesn't deliver the invitation message. In this case, you must update your message template and resend the password with a new `AdminCreateUser` request with a `MessageAction` value of `RESEND`.

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "ClientMetadata": {
    "string" : "string"
  },
  "DesiredDeliveryMediums": [ "string" ],
  "ForceAliasCreation": boolean,
  "MessageAction": "string",
  "TemporaryPassword": "string",
  "UserAttributes": [
    {
      "Name": "string",
      "Value": "string"
    }
  ],
  "Username": "string",
  "UserPoolId": "string",
  "ValidationData": [
    {
      "Name": "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.

ClientMetadata

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

DesiredDeliveryMediums

Specify EMAIL if email will be used to send the welcome message. Specify SMS if the phone number will be used. The default value is SMS. You can specify more than one value.

Type: Array of strings

Valid Values: SMS | EMAIL

Required: No

ForceAliasCreation

This parameter is used only if the `phone_number_verified` or `email_verified` attribute is set to `True`. Otherwise, it is ignored.

If this parameter is set to `True` and the phone number or email address specified in the `UserAttributes` parameter already exists as an alias with a different user, this request migrates the alias from the previous user to the newly-created user. The previous user will no longer be able to log in using that alias.

If this parameter is set to `False`, the API throws an `AliasExistsException` error if the alias already exists. The default value is `False`.

Type: Boolean

Required: No

MessageAction

Set to `RESEND` to resend the invitation message to a user that already exists, and to reset the temporary-password duration with a new temporary password. Set to `SUPPRESS` to suppress sending the message. You can specify only one value.

Type: String

Valid Values: RESEND | SUPPRESS

Required: No

TemporaryPassword

The user's temporary password. This password must conform to the password policy that you specified when you created the user pool.

The exception to the requirement for a password is when your user pool supports passwordless sign-in with email or SMS OTPs. To create a user with no password, omit this parameter or submit a blank value. You can only create a passwordless user when passwordless sign-in is available.

For enabling passwordless factors, see [CreateUserPool:Policies](#) and [UpdateUserPool:Policies](#).

The temporary password is valid only once. To complete the Admin Create User flow, the user must enter the temporary password in the sign-in page, along with a new password to be used in all future sign-ins.

If you don't specify a value, Amazon Cognito generates one for you unless you have passwordless options active for your user pool.

The temporary password can only be used until the user account expiration limit that you set for your user pool. To reset the account after that time limit, you must call `AdminCreateUser` again and specify `RESEND` for the `MessageAction` parameter.

Type: String

Length Constraints: Maximum length of 256.

Pattern: `[\S]+`

Required: No

UserAttributes

An array of name-value pairs that contain user attributes and attribute values to be set for the user to be created. You can create a user without specifying any attributes other than `Username`. However, any attributes that you specify as required (when creating a user pool or in the **Attributes** tab of the console) either you should supply (in your call to `AdminCreateUser`) or the user should supply (when they sign up in response to your welcome message).

For custom attributes, you must prepend the `custom:` prefix to the attribute name.

To send a message inviting the user to sign up, you must specify the user's email address or phone number. You can do this in your call to `AdminCreateUser` or in the **Users** tab of the Amazon Cognito console for managing your user pools.

You must also provide an email address or phone number when you expect the user to do passwordless sign-in with an email or SMS OTP. These attributes must be provided when passwordless options are the only available, or when you don't submit a `TemporaryPassword`.

In your `AdminCreateUser` request, you can set the `email_verified` and `phone_number_verified` attributes to `true`. The following conditions apply:

email

The email address where you want the user to receive their confirmation code and username. You must provide a value for `email` when you want to set `email_verified` to `true`, or if you set `EMAIL` in the `DesiredDeliveryMediums` parameter.

phone_number

The phone number where you want the user to receive their confirmation code and username. You must provide a value for `phone_number` when you want to set `phone_number_verified` to `true`, or if you set `SMS` in the `DesiredDeliveryMediums` parameter.

You can also set attributes verified with [AdminUpdateUserAttributes](#).

Type: Array of [AttributeType](#) objects

Required: No

Username

The value that you want to set as the username sign-in attribute. The following conditions apply to the username parameter.

- The username can't be a duplicate of another username in the same user pool.
- You can't change the value of a username after you create it.
- You can only provide a value if usernames are a valid sign-in attribute for your user pool. If your user pool only supports phone numbers or email addresses as sign-in attributes, Amazon Cognito automatically generates a username value. For more information, see [Customizing sign-in attributes](#).

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}] +`

Required: Yes

UserPoolId

The ID of the user pool where you want to create a user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

ValidationData

Temporary user attributes that contribute to the outcomes of your pre sign-up Lambda trigger. This set of key-value pairs are for custom validation of information that you collect from your users but don't need to retain.

Your Lambda function can analyze this additional data and act on it. Your function can automatically confirm and verify select users or perform external API operations like logging user attributes and validation data to Amazon CloudWatch Logs.

For more information about the pre sign-up Lambda trigger, see [Pre sign-up Lambda trigger](#).

Type: Array of [AttributeType](#) objects

Required: No

Response Syntax

```
{
  "User": {
    "Attributes": [
      {
        "Name": "string",
        "Value": "string"
      }
    ],
    "Enabled": boolean,
    "MFAOptions": [
      {
        "AttributeName": "string",
        "DeliveryMedium": "string"
      }
    ],
    "UserCreateDate": number,
```

```
    "UserLastModifiedDate": number,  
    "Username": "string",  
    "UserStatus": "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.

User

The new user's profile details.

Type: [UserType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

CodeDeliveryFailureException

This exception is thrown when a verification code fails to deliver successfully.

message

The message sent when a verification code fails to deliver successfully.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidPasswordException

This exception is thrown when Amazon Cognito encounters an invalid password.

message

The message returned when Amazon Cognito throws an invalid user password exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the

external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PreconditionNotMetException

This exception is thrown when a precondition is not met.

message

The message returned when a precondition is not met.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UnsupportedUserStateException

The request failed because the user is in an unsupported state.

message

The message returned when the user is in an unsupported state.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UsernameExistsException

This exception is thrown when Amazon Cognito encounters a user name that already exists in the user pool.

message

The message returned when Amazon Cognito throws a user name exists exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

An AdminCreateUser request for for a test user named John.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-east-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminCreateUser
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "UserPoolId": "us-east-1_EXAMPLE",
  "Username": "testuser",
  "DesiredDeliveryMediums": [
    "SMS"
  ],
  "MessageAction": "SUPPRESS",
  "TemporaryPassword": "This-is-my-test-99!",
  "UserAttributes": [
    {
      "Name": "name",
      "Value": "John"
    },
    {
      "Name": "phone_number",
```



```
        "Value": "+12065551212"
      },
      {
        "Name": "email",
        "Value": "testuser@example.com"
      }
    ]
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "User": {
    "Attributes": [
      {
        "Name": "sub",
        "Value": "d16b4aa8-8633-4abd-93b3-5062a8e1b5f8"
      },
      {
        "Name": "name",
        "Value": "John"
      },
      {
        "Name": "phone_number",
        "Value": "+12065551212"
      },
      {
        "Name": "email",
        "Value": "testuser@example.com"
      }
    ],
    "Enabled": true,
    "UserCreateDate": 1689980857.949,
    "UserLastModifiedDate": 1689980857.949,
    "UserStatus": "FORCE_CHANGE_PASSWORD",
    "Username": "testuser"
  }
}
```

```
}  
}
```

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](#)

AdminDeleteUser

Deletes a user profile in your user pool.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "Username": "string",  
  "UserPoolId": "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.

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to delete the user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example operation deletes the user "testuser" from the user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminDeleteUser
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
```

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](#)

AdminDeleteUserAttributes

Deletes attribute values from a user. This operation doesn't affect tokens for existing user sessions. The next ID token that the user receives will no longer have the deleted attributes.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "UserAttributeNames": [ "string" ],  
  "Username": "string",  
  "UserPoolId": "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.

[UserAttributeNames](#)

An array of strings representing the user attribute names you want to delete.

For custom attributes, you must prepend the custom: prefix to the attribute name.

Type: Array of strings

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\t\n\r ]+`

Required: Yes

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to delete user attributes.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example API request deletes the attribute `custom:deliverables` from the user "testuser."

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminDeleteUserAttributes
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "UserAttributeNames": [
    "custom:deliverables"
  ],
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
```

```
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{}
```

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](#)

AdminDisableProviderForUser

Prevents the user from signing in with the specified external (SAML or social) identity provider (IdP). If the user that you want to deactivate is a Amazon Cognito user pools native username + password user, they can't use their password to sign in. If the user to deactivate is a linked external IdP user, any link between that user and an existing user is removed. When the external user signs in again, and the user is no longer attached to the previously linked `DestinationUser`, the user must create a new user account.

For information about linking users, see [AdminLinkProviderForUser](#).

The value of `ProviderName` must match the name of a user pool IdP.

To deactivate a local user, set `ProviderName` to `Cognito` and the `ProviderAttributeName` to `Cognito_Subject`. The `ProviderAttributeValue` must be user's local username.

The `ProviderAttributeName` must always be `Cognito_Subject` for social IdPs. The `ProviderAttributeValue` must always be the exact subject that was used when the user was originally linked as a source user.

For de-linking a SAML identity, there are two scenarios. If the linked identity has not yet been used to sign in, the `ProviderAttributeName` and `ProviderAttributeValue` must be the same values that were used for the `SourceUser` when the identities were originally linked using `AdminLinkProviderForUser` call. This is also true if the linking was done with `ProviderAttributeName` set to `Cognito_Subject`. If the user has already signed in, the `ProviderAttributeName` must be `Cognito_Subject` and `ProviderAttributeValue` must be the `NameID` from their SAML assertion.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "User": {  
    "ProviderAttributeName": "string",  
    "ProviderAttributeValue": "string",  
    "ProviderName": "string"  
  },  
  "UserPoolId": "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.

User

The user profile that you want to delete a linked identity from.

Type: [ProviderUserIdentifierType](#) object

Required: Yes

UserPoolId

The ID of the user pool where you want to delete the user's linked identities.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#).

AliasExistsException

This exception is thrown when a user tries to confirm the account with an email address or phone number that has already been supplied as an alias for a different user profile. This exception indicates that an account with this email address or phone already exists in a user pool that you've configured to use email address or phone number as a sign-in alias.

message

The message that Amazon Cognito sends to the user when the value of an alias attribute is already linked to another user profile.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

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](#)

AdminDisableUser

Deactivates a user profile and revokes all access tokens for the user. A deactivated user can't sign in, but still appears in the responses to `ListUsers` API requests.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "Username": "string",
  "UserPoolId": "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.

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to disable the user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example API request deactivates the user "testuser."

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminDisableUser
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{}
```

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](#)

AdminEnableUser

Activates sign-in for a user profile that previously had sign-in access disabled.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "Username": "string",  
  "UserPoolId": "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.

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to activate sign-in for the user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example API request activates the user "testuser."

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminEnableUser
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{}
```

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](#)

AdminForgetDevice

Forgets, or deletes, a remembered device from a user's profile. After you forget the device, the user can no longer complete device authentication with that device and when applicable, must submit MFA codes again. For more information, see [Working with devices](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "DeviceKey": "string",
  "Username": "string",
  "UserPoolId": "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.

[DeviceKey](#)

The key ID of the device that you want to delete.

You can get device keys in the response to an [AdminListDevices](#) request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-f-]+`

Required: Yes

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where the device owner is a user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example API request deletes a remembered device for the user "testuser."

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminForgetDevice
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
  "UserPoolId": "us-west-2_EXAMPLE",
```

```
"Username": "testuser"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
```

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](#)

AdminGetDevice

Given the device key, returns details for a user's device. For more information, see [Working with devices](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "DeviceKey": "string",  
  "Username": "string",  
  "UserPoolId": "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.

DeviceKey

The key of the device that you want to delete.

You can get device IDs in the response to an [AdminListDevices](#) request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-f-]+`

Required: Yes

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If `username` isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where the device owner is a user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "Device": {
    "DeviceAttributes": [
      {
        "Name": "string",
        "Value": "string"
      }
    ],
    "DeviceCreateDate": number,
    "DeviceKey": "string",
    "DeviceLastAuthenticatedDate": number,
```

```
    "DeviceLastModifiedDate": 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.

Device

Details of the requested device. Includes device information, last-accessed and created dates, and the device key.

Type: [DeviceType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example API request retrieves information about a device that belongs to the user "testuser."

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminGetDevice
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "Device": {
    "DeviceAttributes": [
      {
        "Name": "device_status",
        "Value": "valid"
      },
      {
        "Name": "device_name",
        "Value": "Dart-device"
      },
      {
        "Name": "dev:device_arn",
        "Value": "arn:aws:cognito-idp:us-west-2:123456789012:owner/testuser.us-west-2_EXAMPLE/device/us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
      }
    ]
  }
}
```

```
{
  "Name": "dev:device_owner",
  "Value": "testuser.us-west-2_EXAMPLE"
},
{
  "Name": "last_ip_used",
  "Value": "192.0.2.1"
},
{
  "Name": "dev:device_remembered_status",
  "Value": "remembered"
},
{
  "Name": "dev:device_sdk",
  "Value": "aws-sdk-unknown-unknown"
}
],
"DeviceCreateDate": 1715100742.022,
"DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
"DeviceLastAuthenticatedDate": 1715100742.0,
"DeviceLastModifiedDate": 1715100742.022
}
}
```

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](#)

AdminGetUser

Given a username, returns details about a user profile in a user pool. You can specify alias attributes in the Username request parameter.

This operation contributes to your monthly active user (MAU) count for the purpose of billing.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "Username": "string",  
  "UserPoolId": "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.

[Username](#)

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to get information about the user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "Enabled": boolean,
  "MFAOptions": [
    {
      "AttributeName": "string",
      "DeliveryMedium": "string"
    }
  ],
  "PreferredMfaSetting": "string",
  "UserAttributes": [
    {
      "Name": "string",
      "Value": "string"
    }
  ],
  "UserCreateDate": number,
  "UserLastModifiedDate": number,
  "UserMFASettingList": [ "string" ],
  "Username": "string",
  "UserStatus": "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.

Enabled

Indicates whether the user is activated for sign-in.

The [AdminDisableUser](#) and [AdminEnableUser](#) API operations deactivate and activate user sign-in, respectively.

Type: Boolean

MFAOptions

This response parameter is no longer supported. It provides information only about SMS MFA configurations. It doesn't provide information about time-based one-time password (TOTP) software token MFA configurations. To look up information about either type of MFA configuration, use `UserMFASettingList` instead.

Type: Array of [MFAOptionType](#) objects

PreferredMfaSetting

The user's preferred MFA. Users can prefer SMS message, email message, or TOTP MFA.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

UserAttributes

An array of name-value pairs of user attributes and their values, for example "email": "testuser@example.com".

Type: Array of [AttributeType](#) objects

UserCreateDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

UserLastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

UserMFASettingList

The MFA options that are activated for the user. The possible values in this list are SMS_MFA, EMAIL_OTP, and SOFTWARE_TOKEN_MFA.

You can change the MFA preference for users who have more than one available MFA factor with [AdminSetUserMFAPreference](#) or [SetUserMFAPreference](#).

Type: Array of strings

Length Constraints: Minimum length of 0. Maximum length of 131072.

Username

The username of the user that you requested.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]`+

UserStatus

The user's status. Can be one of the following:

- UNCONFIRMED - User has been created but not confirmed.
- CONFIRMED - User has been confirmed.
- UNKNOWN - User status isn't known.
- RESET_REQUIRED - User is confirmed, but the user must request a code and reset their password before they can sign in.
- FORCE_CHANGE_PASSWORD - The user is confirmed and the user can sign in using a temporary password, but on first sign-in, the user must change their password to a new value before doing anything else.

- **EXTERNAL_PROVIDER** - The user signed in with a third-party identity provider.

Type: String

Valid Values: UNCONFIRMED | CONFIRMED | ARCHIVED | COMPROMISED | UNKNOWN | RESET_REQUIRED | FORCE_CHANGE_PASSWORD | EXTERNAL_PROVIDER

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example API request gets user details for the user "testuser."

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminGetUser
```

```
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "Enabled": true,
  "UserAttributes": [
    {
      "Name": "sub",
      "Value": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
    {
      "Name": "identities",
      "Value": "[{\"userId\":\"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222\",
\\\"providerName\\\":\\\"SignInWithApple\\\",\\\"providerType\\\":\\\"SignInWithApple\\\",\\\"issuer\\\":null,\\\"primary\\\":false,\\\"dateCreated\\\":1701125599632}]"
    },
    {
      "Name": "email_verified",
      "Value": "true"
    },
    {
      "Name": "custom:deliverables",
      "Value": "project-111222"
    },
    {
      "Name": "name",
      "Value": "John"
    }
  ]
}
```

```
    },
    {
      "Name": "phone_number_verified",
      "Value": "true"
    },
    {
      "Name": "phone_number",
      "Value": "+12065551212"
    },
    {
      "Name": "preferred_username",
      "Value": "John Doe"
    },
    {
      "Name": "locale",
      "Value": "EMEA"
    },
    {
      "Name": "email",
      "Value": "testuser@example.com"
    }
  ],
  "UserCreateDate": 1.682955829578E9,
  "UserLastModifiedDate": 1.722380161794E9,
  "UserStatus": "CONFIRMED",
  "Username": "testuser"
}
```

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](#)

AdminInitiateAuth

Starts sign-in for applications with a server-side component, for example a traditional web application. This operation specifies the authentication flow that you'd like to begin. The authentication flow that you specify must be supported in your app client configuration. For more information about authentication flows, see [Authentication flows](#).

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
```

```
{
  "AnalyticsMetadata": {
    "AnalyticsEndpointId": "string"
  },
  "AuthFlow": "string",
  "AuthParameters": {
    "string" : "string"
  },
  "ClientId": "string",
  "ClientMetadata": {
    "string" : "string"
  },
  "ContextData": {
    "EncodedData": "string",
    "HttpHeaders": [
      {
        "headerName": "string",
        "headerValue": "string"
      }
    ],
    "IpAddress": "string",
    "ServerName": "string",
    "ServerPath": "string"
  },
  "Session": "string",
  "UserPoolId": "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.

[AnalyticsMetadata](#)

Information that supports analytics outcomes with Amazon Pinpoint, including the user's endpoint ID. The endpoint ID is a destination for Amazon Pinpoint push notifications, for example a device identifier, email address, or phone number.

Type: [AnalyticsMetadataType](#) object

Required: No

AuthFlow

The authentication flow that you want to initiate. Each AuthFlow has linked AuthParameters that you must submit. The following are some example flows.

Include the required [AdminInitiateAuth:AuthParameters](#) for the flow that you choose.

USER_AUTH

The entry point for [choice-based authentication](#) with passwords, one-time passwords, and WebAuthn authenticators. Request a preferred authentication type or review available authentication types. From the offered authentication types, select one in a challenge response and then authenticate with that method in an additional challenge response. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

USER_SRP_AUTH

Username-password authentication with the Secure Remote Password (SRP) protocol. For more information, see [Use SRP password verification in custom authentication flow](#).

REFRESH_TOKEN_AUTH and REFRESH_TOKEN

Receive new ID and access tokens when you pass a REFRESH_TOKEN parameter with a valid refresh token as the value. For more information, see [Using the refresh token](#).

CUSTOM_AUTH

Custom authentication with Lambda triggers. For more information, see [Custom authentication challenge Lambda triggers](#).

ADMIN_USER_PASSWORD_AUTH

Server-side username-password authentication with the password sent directly in the request. For more information about client-side and server-side authentication, see [SDK authorization models](#).

USER_PASSWORD_AUTH is a flow type of [InitiateAuth](#) and isn't valid for AdminInitiateAuth.

Type: String

Valid Values: USER_SRP_AUTH | REFRESH_TOKEN_AUTH | REFRESH_TOKEN
| CUSTOM_AUTH | ADMIN_NO_SRP_AUTH | USER_PASSWORD_AUTH |
ADMIN_USER_PASSWORD_AUTH | USER_AUTH

Required: Yes

AuthParameters

The authentication parameters. These are inputs corresponding to the AuthFlow that you're invoking.

The following are some authentication flows and their parameters. Add a SECRET_HASH parameter if your app client has a client secret. Add DEVICE_KEY if you want to bypass multi-factor authentication with a remembered device.

USER_AUTH

- USERNAME (required)
- PREFERRED_CHALLENGE. If you don't provide a value for PREFERRED_CHALLENGE, Amazon Cognito responds with the AvailableChallenges parameter that specifies the available sign-in methods.

USER_SRP_AUTH

- USERNAME (required)
- SRP_A (required)

ADMIN_USER_PASSWORD_AUTH

- USERNAME (required)
- PASSWORD (required)

REFRESH_TOKEN_AUTH/REFRESH_TOKEN

- REFRESH_TOKEN(required)

CUSTOM_AUTH

- USERNAME (required)
- ChallengeName: SRP_A (when preceding custom authentication with SRP authentication)
- SRP_A: (An SRP_A value) (when preceding custom authentication with SRP authentication)

For more information about SECRET_HASH, see [Computing secret hash values](#). For information about DEVICE_KEY, see [Working with user devices in your user pool](#).

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ClientId

The ID of the app client where the user wants to sign in.

Type: String

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

Pattern: `[\w+]`

Required: Yes

ClientMetadata

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

The `ClientMetadata` value is passed as input to the functions for only the following triggers:

- Pre signup
- Pre authentication
- User migration

This request also invokes the functions for the following triggers, but doesn't pass `ClientMetadata`:

- Post authentication

- Custom message
- Pre token generation
- Create auth challenge
- Define auth challenge
- Custom email sender
- Custom SMS sender

 Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ContextData

Contextual data about your user session like the device fingerprint, IP address, or location. Amazon Cognito threat protection evaluates the risk of an authentication event based on the context that your app generates and passes to Amazon Cognito when it makes API requests.

For more information, see [Collecting data for threat protection in applications](#).

Type: [ContextDataType](#) object

Required: No

Session

The optional session ID from a `ConfirmSignUp` API request. You can sign in a user directly from the sign-up process with an `AuthFlow` of `USER_AUTH` and `AuthParameters` of `EMAIL_OTP` or `SMS_OTP`, depending on how your user pool sent the confirmation-code message.

Type: String

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

Required: No

UserPoolId

The ID of the user pool where the user wants to sign in.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "AuthenticationResult": {
    "AccessToken": "string",
    "ExpiresIn": number,
    "IdToken": "string",
    "NewDeviceMetadata": {
      "DeviceGroupKey": "string",
      "DeviceKey": "string"
    },
    "RefreshToken": "string",
    "TokenType": "string"
  },
  "AvailableChallenges": [ "string" ],
```

```
"ChallengeName": "string",
"ChallengeParameters": {
  "string" : "string"
},
"Session": "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.

AuthenticationResult

The outcome of successful authentication. This is only returned if the user pool has no additional challenges to return. If Amazon Cognito returns another challenge, the response includes ChallengeName, ChallengeParameters, and Session so that your user can answer the challenge.

Type: [AuthenticationResultType](#) object

AvailableChallenges

This response parameter lists the available authentication challenges that users can select from in [choice-based authentication](#). For example, they might be able to choose between passkey authentication, a one-time password from an SMS message, and a traditional password.

Type: Array of strings

Valid Values: SMS_MFA | EMAIL_OTP | SOFTWARE_TOKEN_MFA | SELECT_MFA_TYPE | MFA_SETUP | PASSWORD_VERIFIER | CUSTOM_CHALLENGE | SELECT_CHALLENGE | DEVICE_SRP_AUTH | DEVICE_PASSWORD_VERIFIER | ADMIN_NO_SRP_AUTH | NEW_PASSWORD_REQUIRED | SMS_OTP | PASSWORD | WEB_AUTHN | PASSWORD_SRP

ChallengeName

The name of the challenge that you're responding to with this call. This is returned in the AdminInitiateAuth response if you must pass another challenge.

Possible challenges include the following:

Note

All of the following challenges require USERNAME and, when the app client has a client secret, SECRET_HASH in the parameters. Include a DEVICE_KEY for device authentication.

- **WEB_AUTHN:** Respond to the challenge with the results of a successful authentication with a WebAuthn authenticator, or passkey, as CREDENTIAL. Examples of WebAuthn authenticators include biometric devices and security keys.
- **PASSWORD:** Respond with the user's password as PASSWORD.
- **PASSWORD_SRP:** Respond with the initial SRP secret as SRP_A.
- **SELECT_CHALLENGE:** Respond with a challenge selection as ANSWER. It must be one of the challenge types in the AvailableChallenges response parameter. Add the parameters of the selected challenge, for example USERNAME and SMS_OTP.
- **SMS_MFA:** Respond with the code that your user pool delivered in an SMS message, as SMS_MFA_CODE
- **EMAIL_MFA:** Respond with the code that your user pool delivered in an email message, as EMAIL_MFA_CODE
- **EMAIL_OTP:** Respond with the code that your user pool delivered in an email message, as EMAIL_OTP_CODE .
- **SMS_OTP:** Respond with the code that your user pool delivered in an SMS message, as SMS_OTP_CODE.
- **PASSWORD_VERIFIER:** Respond with the second stage of SRP secrets as PASSWORD_CLAIM_SIGNATURE, PASSWORD_CLAIM_SECRET_BLOCK, and TIMESTAMP.
- **CUSTOM_CHALLENGE:** This is returned if your custom authentication flow determines that the user should pass another challenge before tokens are issued. The parameters of the challenge are determined by your Lambda function and issued in the ChallengeParameters of a challenge response.
- **DEVICE_SRP_AUTH:** Respond with the initial parameters of device SRP authentication. For more information, see [Signing in with a device](#).
- **DEVICE_PASSWORD_VERIFIER:** Respond with PASSWORD_CLAIM_SIGNATURE, PASSWORD_CLAIM_SECRET_BLOCK, and TIMESTAMP after client-side SRP calculations. For more information, see [Signing in with a device](#).

- **NEW_PASSWORD_REQUIRED:** For users who are required to change their passwords after successful first login. Respond to this challenge with **NEW_PASSWORD** and any required attributes that Amazon Cognito returned in the **requiredAttributes** parameter. You can also set values for attributes that aren't required by your user pool and that your app client can write.

Amazon Cognito only returns this challenge for users who have temporary passwords. When you create passwordless users, you must provide values for all required attributes.

 Note

In a **NEW_PASSWORD_REQUIRED** challenge response, you can't modify a required attribute that already has a value. In **AdminRespondToAuthChallenge** or **RespondToAuthChallenge**, set a value for any keys that Amazon Cognito returned in the **requiredAttributes** parameter, then use the **AdminUpdateUserAttributes** or **UpdateUserAttributes** API operation to modify the value of any additional attributes.

- **MFA_SETUP:** For users who are required to setup an MFA factor before they can sign in. The MFA types activated for the user pool will be listed in the challenge parameters **MFAS_CAN_SETUP** value.

To set up time-based one-time password (TOTP) MFA, use the session returned in this challenge from **InitiateAuth** or **AdminInitiateAuth** as an input to **AssociateSoftwareToken**. Then, use the session returned by **VerifySoftwareToken** as an input to **RespondToAuthChallenge** or **AdminRespondToAuthChallenge** with challenge name **MFA_SETUP** to complete sign-in.

To set up SMS or email MFA, collect a **phone_number** or **email** attribute for the user. Then restart the authentication flow with an **InitiateAuth** or **AdminInitiateAuth** request.

Type: String

Valid Values: **SMS_MFA** | **EMAIL_OTP** | **SOFTWARE_TOKEN_MFA** | **SELECT_MFA_TYPE** | **MFA_SETUP** | **PASSWORD_VERIFIER** | **CUSTOM_CHALLENGE** | **SELECT_CHALLENGE** | **DEVICE_SRP_AUTH** | **DEVICE_PASSWORD_VERIFIER** | **ADMIN_NO_SRP_AUTH** | **NEW_PASSWORD_REQUIRED** | **SMS_OTP** | **PASSWORD** | **WEB_AUTHN** | **PASSWORD_SRP**

ChallengeParameters

The parameters of an authentication challenge. Amazon Cognito returns challenge parameters as a guide to the responses your user or application must provide for the returned ChallengeName. Calculate responses to the challenge parameters and pass them in the ChallengeParameters of AdminRespondToAuthChallenge.

All challenges require USERNAME and, when the app client has a client secret, SECRET_HASH.

In SRP challenges, Amazon Cognito returns the username attribute in USER_ID_FOR_SRP instead of any email address, preferred username, or phone number alias that you might have specified in your AdminInitiateAuth request. You must use the username and not an alias in the ChallengeResponses of your challenge response.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Session

The session that must be passed to challenge-response requests. If an AdminInitiateAuth or AdminRespondToAuthChallenge API request results in another authentication challenge, Amazon Cognito returns a session ID and the parameters of the next challenge. Pass this session ID in the Session parameter of AdminRespondToAuthChallenge.

Type: String

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

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

MFAMethodNotFoundException

This exception is thrown when Amazon Cognito can't find a multi-factor authentication (MFA) method.

message

The message returned when Amazon Cognito throws an MFA method not found exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UnsupportedOperationException

Exception that is thrown when you attempt to perform an operation that isn't enabled for the user pool client.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request signs in the user "testuser" to an app client with a client secret. It includes context data for advanced security features and ClientMetadata for Lambda triggers. The device key and device group key in the response indicate that this user pool supports the device-remembering feature.

Sample Request

```
POST HTTP/1.1
```

```
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminInitiateAuth
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AuthFlow": "ADMIN_USER_PASSWORD_AUTH",
  "ClientId": "1example23456789",
  "UserPoolId": "us-west-2_EXAMPLE",
  "AuthParameters": {
    "USERNAME": "testuser",
    "PASSWORD": "TestUserPassword1=",
    "SECRET_HASH": "cKtx2L2fvV1FeAbk3iUPgCyXY+5B0It00ItxhFaLkeA="
  },
  "ContextData": {
    "EncodedData": "VGhpc0lzTXlFbmNvZGVkRGF0YQ",
    "HttpHeaders": [
      {
        "headerName": "Referer",
        "headerValue": "https://home.example.com"
      }
    ],
    "IpAddress": "192.0.2.100",
    "ServerName": "auth.example.com",
    "ServerPath": "/web/private/program.html"
  },
  "ClientMetadata": {
    "MyTestKey": "MyTestValue"
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
```



```
"AuthenticationResult": {
  "AccessToken": "eyJraACCESSEXAMPLE...",
  "ExpiresIn": 3600,
  "IdToken": "eyJraIDEXAMPLE...",
  "NewDeviceMetadata": {
    "DeviceGroupKey": "-v7w9UcY6",
    "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
  },
  "RefreshToken": "eyJjREFRESHEXAMPLE...",
  "TokenType": "Bearer"
},
"ChallengeParameters": {}
}
```

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](#)

AdminLinkProviderForUser

Links an existing user account in a user pool, or `DestinationUser`, to an identity from an external IdP, or `SourceUser`, based on a specified attribute name and value from the external IdP.

This operation connects a local user profile with a user identity who hasn't yet signed in from their third-party IdP. When the user signs in with their IdP, they get access-control configuration from the local user profile. Linked local users can also sign in with SDK-based API operations like `InitiateAuth` after they sign in at least once through their IdP. For more information, see [Linking federated users](#).

Note

The maximum number of federated identities linked to a user is five.

Important

Because this API allows a user with an external federated identity to sign in as a local user, it is critical that it only be used with external IdPs and linked attributes that you trust.

See also [AdminDisableProviderForUser](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
```

```
"DestinationUser": {
  "ProviderAttributeName": "string",
  "ProviderAttributeValue": "string",
  "ProviderName": "string"
},
"SourceUser": {
  "ProviderAttributeName": "string",
  "ProviderAttributeValue": "string",
  "ProviderName": "string"
},
"UserPoolId": "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.

[DestinationUser](#)

The existing user in the user pool that you want to assign to the external IdP user account. This user can be a local (Username + Password) Amazon Cognito user pools user or a federated user (for example, a SAML or Facebook user). If the user doesn't exist, Amazon Cognito generates an exception. Amazon Cognito returns this user when the new user (with the linked IdP attribute) signs in.

For a native username + password user, the `ProviderAttributeValue` for the `DestinationUser` should be the username in the user pool. For a federated user, it should be the provider-specific `user_id`.

The `ProviderAttributeName` of the `DestinationUser` is ignored.

The `ProviderName` should be set to `Cognito` for users in Cognito user pools.

Important

All attributes in the `DestinationUser` profile must be mutable. If you have assigned the user any immutable custom attributes, the operation won't succeed.

Type: [ProviderUserIdentifierType](#) object

Required: Yes

SourceUser

An external IdP account for a user who doesn't exist yet in the user pool. This user must be a federated user (for example, a SAML or Facebook user), not another native user.

If the `SourceUser` is using a federated social IdP, such as Facebook, Google, or Login with Amazon, you must set the `ProviderAttributeName` to `Cognito_Subject`. For social IdPs, the `ProviderName` will be Facebook, Google, or LoginWithAmazon, and Amazon Cognito will automatically parse the Facebook, Google, and Login with Amazon tokens for `id`, `sub`, and `user_id`, respectively. The `ProviderAttributeValue` for the user must be the same value as the `id`, `sub`, or `user_id` value found in the social IdP token.

For OIDC, the `ProviderAttributeName` can be any mapped value from a claim in the ID token, or that your app retrieves from the `userInfo` endpoint. For SAML, the `ProviderAttributeName` can be any mapped value from a claim in the SAML assertion.

The following additional considerations apply to `SourceUser` for OIDC and SAML providers.

- You must map the claim to a user pool attribute in your IdP configuration, and set the user pool attribute name as the value of `ProviderAttributeName` in your `AdminLinkProviderForUser` request. For example, `email`.
- When you set `ProviderAttributeName` to `Cognito_Subject`, Amazon Cognito will automatically parse the default unique identifier found in the subject from the IdP token.

Type: [ProviderUserIdentifierType](#) object

Required: Yes

UserPoolId

The ID of the user pool where you want to link a federated identity.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#).

AliasExistsException

This exception is thrown when a user tries to confirm the account with an email address or phone number that has already been supplied as an alias for a different user profile. This exception indicates that an account with this email address or phone already exists in a user pool that you've configured to use email address or phone number as a sign-in alias.

message

The message that Amazon Cognito sends to the user when the value of an alias attribute is already linked to another user profile.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example links a Facebook user to the user pool user "adminlink-testuser." The user's unique identifier with Facebook is represented in the value of `ProviderAttributeValue`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminLinkProviderForUser
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "DestinationUser": {
    "ProviderAttributeValue": "adminlink-testuser",
    "ProviderName": "Cognito"
  },
  "SourceUser": {
    "ProviderAttributeName": "Cognito_Subject",
    "ProviderAttributeValue": "123456789012345",
    "ProviderName": "Facebook"
  },
  "UserPoolId": "us-west-2_EXAMPLE"}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

Example

The following example links a Google user to the user pool user "adminlink-testuser." The user's unique identifier with Google is represented in the value of `ProviderAttributeValue`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminLinkProviderForUser
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "DestinationUser": {
    "ProviderAttributeValue": "adminlink-testuser",
    "ProviderName": "Cognito"
  },
  "SourceUser": {
    "ProviderAttributeName": "Cognito_Subject",
    "ProviderAttributeValue": "5432109876543210",
    "ProviderName": "Google"
  },
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```


Example

The following example links a Login With Amazon user to the user pool user "adminlink-testuser." The user's unique identifier with Amazon is represented in the value of `ProviderAttributeValue`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminLinkProviderForUser
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "DestinationUser": {
    "ProviderAttributeValue": "adminlink-testuser",
    "ProviderName": "Cognito"
  },
  "SourceUser": {
    "ProviderAttributeName": "Cognito_Subject",
    "ProviderAttributeValue": "amzn1.account.AFALI...",
    "ProviderName": "LoginWithAmazon"
  },
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```


Example

The following example links a user from OIDC provider "MyOIDCProvider" to the user pool user "adminlink-testuser." This request links the local user to an IdP user that has a `preferred_username` attribute of `testuser@example.com`. For this user to sync, your application must request scopes that return the `preferred_username` attribute from the IdP.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminLinkProviderForUser
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "DestinationUser": {
    "ProviderAttributeValue": "adminlink-testuser",
    "ProviderName": "Cognito"
  },
  "SourceUser": {
    "ProviderAttributeName": "preferred_username",
    "ProviderAttributeValue": "testuser@example.com",
    "ProviderName": "MyOIDCProvider"
  },
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

Example

The following example links a user from SAML 2.0 provider "MySAMLProvider" to the user pool user "adminlink-testuser." This request links the local user to an IdP user that has a `email` attribute of `testuser@example.com`. For this user to sync, your application must receive an `email` claim in the SAML assertion.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminLinkProviderForUser
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "DestinationUser": {
    "ProviderAttributeValue": "adminlink-testuser",
    "ProviderName": "Cognito"
  },
  "SourceUser": {
    "ProviderAttributeName": "email",
    "ProviderAttributeValue": "testuser@example.com",
    "ProviderName": "MySAMLProvider"
  },
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

AdminListDevices

Lists a user's registered devices. Remembered devices are used in authentication services where you offer a "Remember me" option for users who you want to permit to sign in without MFA from a trusted device. Users can bypass MFA while your application performs device SRP authentication on the back end. For more information, see [Working with devices](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "Limit": number,
  "PaginationToken": "string",
  "Username": "string",
  "UserPoolId": "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.

Limit

The maximum number of devices that you want Amazon Cognito to return in the response.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 60.

Required: No

PaginationToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

Required: No

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If `username` isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where the device owner is a user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "Devices": [
    {
      "DeviceAttributes": [
        {
          "Name": "string",
          "Value": "string"
        }
      ],
      "DeviceCreateDate": number,
      "DeviceKey": "string",
      "DeviceLastAuthenticatedDate": number,
      "DeviceLastModifiedDate": number
    }
  ],
  "PaginationToken": "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.

Devices

An array of devices and their information. Each entry that's returned includes device information, last-accessed and created dates, and the device key.

Type: Array of [DeviceType](#) objects

PaginationToken

The identifier that Amazon Cognito returned with the previous request to this operation. When you include a pagination token in your request, Amazon Cognito returns the next set of items in the list. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example API request retrieves information about the first two devices that belong to the user "testuser."

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminListDevices
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
```

Content-Length: <PayloadSizeBytes>

```
{
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser" ,
  "Limit": 2
}
```

Sample Response

HTTP/1.1 200 OK

Date: Tue, 13 Jun 2023 20:00:59 GMT

Content-Type: application/x-amz-json-1.0

Content-Length: <PayloadSizeBytes>

x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111

Connection: keep-alive

```
{
  "Devices": [
    {
      "DeviceAttributes": [
        {
          "Name": "device_status",
          "Value": "valid"
        },
        {
          "Name": "device_name",
          "Value": "Dart-device"
        },
        {
          "Name": "dev:device_arn",
          "Value": "arn:aws:cognito-idp:us-west-2:123456789012:owner/testuser.us-west-2_EXAMPLE/device/us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
        },
        {
          "Name": "dev:device_owner",
          "Value": "testuser.us-west-2_EXAMPLE"
        },
        {
          "Name": "last_ip_used",
          "Value": "192.0.2.1"
        },
        {
          "Name": "dev:device_remembered_status",
```

```
    "Value": "remembered"
  },
  {
    "Name": "dev:device_sdk",
    "Value": "aws-sdk-unknown-unknown"
  }
],
"DeviceCreateDate": 1715100742.022,
"DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
"DeviceLastAuthenticatedDate": 1715100742.0,
"DeviceLastModifiedDate": 1715100742.022
},
{
  "DeviceAttributes": [
    {
      "Name": "device_status",
      "Value": "valid"
    },
    {
      "Name": "device_name",
      "Value": "Mobile-device"
    },
    {
      "Name": "dev:device_arn",
      "Value": "arn:aws:cognito-idp:us-west-2:123456789012:owner/testuser.us-west-2_EXAMPLE/device/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
    {
      "Name": "dev:device_owner",
      "Value": "testuser.us-west-2_EXAMPLE"
    },
    {
      "Name": "last_ip_used",
      "Value": "192.0.2.99"
    },
    {
      "Name": "dev:device_remembered_status",
      "Value": "remembered"
    },
    {
      "Name": "dev:device_sdk",
      "Value": "aws-sdk-unknown-unknown"
    }
  ]
},
```

```
"DeviceCreateDate": 1715100742.022,  
"DeviceKey": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",  
"DeviceLastAuthenticatedDate": 1715100742.0,  
"DeviceLastModifiedDate": 1715100742.022  
}  
]  
}
```

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](#)

AdminListGroupsForUser

Lists the groups that a user belongs to. User pool groups are identifiers that you can reference from the contents of ID and access tokens, and set preferred IAM roles for identity-pool authentication. For more information, see [Adding groups to a user pool](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "Limit": number,  
  "NextToken": "string",  
  "Username": "string",  
  "UserPoolId": "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.

Limit

The maximum number of groups that you want Amazon Cognito to return in the response.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 60.

Required: No

NextToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\S]+`

Required: No

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to view a user's groups.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "Groups": [
    {
      "CreationDate": number,
      "Description": "string",
      "GroupName": "string",
      "LastModifiedDate": number,
      "Precedence": number,
      "RoleArn": "string",
      "UserPoolId": "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.

Groups

An array of groups and information about them.

Type: Array of [GroupType](#) objects

NextToken

The identifier that Amazon Cognito returned with the previous request to this operation. When you include a pagination token in your request, Amazon Cognito returns the next set of items in the list. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\S]+`

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request returns the first two groups for the user "testuser." Note that one group has no description and another has no IAM role or precedence assigned. This operation only returns group properties that are configured.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminListGroupsForUser
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE",
```

```
"Username": "testuser",
"Limit": 2
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "Groups": [
    {
      "CreationDate": 1712262633.88,
      "Description": "My first example group",
      "GroupName": "MyExampleGroup1",
      "LastModifiedDate": 1712262633.88,
      "UserPoolId": "us-west-2_EXAMPLE"
    },
    {
      "CreationDate": 1611685503.954,
      "GroupName": "MyExampleGroup2",
      "LastModifiedDate": 1697211218.305,
      "Precedence": 7,
      "RoleArn": "arn:aws:iam::123456789012:role/example-cognito-role",
      "UserPoolId": "us-west-2_EXAMPLE"
    }
  ]
}
```

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](#)

AdminListUserAuthEvents

Requests a history of user activity and any risks detected as part of Amazon Cognito threat protection. For more information, see [Viewing user event history](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "MaxResults": number,  
  "NextToken": "string",  
  "Username": "string",  
  "UserPoolId": "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.

MaxResults

The maximum number of authentication events to return. Returns 60 events if you set `MaxResults` to 0, or if you don't include a `MaxResults` parameter.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 60.

Required: No

NextToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\S]+`

Required: No

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If `username` isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The Id of the user pool that contains the user profile with the logged events.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "AuthEvents": [
    {
      "ChallengeResponses": [
        {
          "ChallengeName": "string",
          "ChallengeResponse": "string"
        }
      ],
      "CreationDate": number,
      "EventContextData": {
        "City": "string",
        "Country": "string",
        "DeviceName": "string",
        "IpAddress": "string",
        "Timezone": "string"
      },
      "EventFeedback": {
        "FeedbackDate": number,
        "FeedbackValue": "string",
        "Provider": "string"
      },
      "EventId": "string",
      "EventResponse": "string",
      "EventRisk": {
        "CompromisedCredentialsDetected": boolean,
        "RiskDecision": "string",
        "RiskLevel": "string"
      },
      "EventType": "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.

AuthEvents

The response object. It includes the EventID, EventType, CreationDate, EventRisk, and EventResponse.

Type: Array of [AuthEventType](#) objects

NextToken

The identifier that Amazon Cognito returned with the previous request to this operation. When you include a pagination token in your request, Amazon Cognito returns the next set of items in the list. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\S]+`

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

UserPoolAddOnNotEnabledException

This exception is thrown when user pool add-ons aren't enabled.

HTTP Status Code: 400

Examples

Example

The following example returns the two most recent advanced security features events for the user "testuser."

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminListUserAuthEvents
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser",
  "MaxResults": 2
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "AuthEvents": [
    {
      "ChallengeResponses": [
        {
          "ChallengeName": "Password",
          "ChallengeResponse": "Success"
        }
      ],
      "CreationDate": 1.7232229982E9,
      "EventContextData": {
```

```
        "City": "null",
        "Country": "United States",
        "IpAddress": "192.0.2.1"
    },
    "EventId": "7875548a-bd00-490a-93b8-fa36fe42a3e0",
    "EventResponse": "Pass",
    "EventRisk": {
        "CompromisedCredentialsDetected": false,
        "RiskDecision": "AccountTakeover",
        "RiskLevel": "Medium"
    },
    "EventType": "SignIn"
},
{
    "ChallengeResponses": [
        {
            "ChallengeName": "Password",
            "ChallengeResponse": "Success"
        }
    ],
    "CreationDate": 1.723136049929E9,
    "EventContextData": {
        "City": "Loughborough",
        "Country": "United Kingdom",
        "DeviceName": "Other, Other",
        "IpAddress": "192.0.2.99"
    },
    "EventId": "768d375c-ee6c-435e-a005-25c4981565c3",
    "EventResponse": "Pass",
    "EventRisk": {
        "CompromisedCredentialsDetected": false,
        "RiskDecision": "AccountTakeover",
        "RiskLevel": "Low"
    },
    "EventType": "SignIn"
}
],
"NextToken": "768d375c-ee6c-435e-a005-25c4981565c3#2024-08-08T16:54:09.929Z"
}
```

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](#)

AdminRemoveUserFromGroup

Given a username and a group name, removes them from the group. User pool groups are identifiers that you can reference from the contents of ID and access tokens, and set preferred IAM roles for identity-pool authentication. For more information, see [Adding groups to a user pool](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "GroupName": "string",
  "Username": "string",
  "UserPoolId": "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.

GroupName

The name of the group that you want to remove the user from, for example MyTestGroup.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]`+

Required: Yes

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]`+

Required: Yes

UserPoolId

The ID of the user pool that contains the group and the user that you want to remove.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]`+

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example removes the user "testuser" from the group "MyExampleGroup1."

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminRemoveUserFromGroup
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "GroupName": "MyExampleGroup1",
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
```


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](#)

AdminResetUserPassword

Begins the password reset process. Sets the requested user's account into a `RESET_REQUIRED` status, and sends them a password-reset code. Your user pool also sends the user a notification with a reset code and the information that their password has been reset. At sign-in, your application or the managed login session receives a challenge to complete the reset by confirming the code and setting a new password.

This operation is the administrative API equivalent to [ForgotPassword](#).

This operation deactivates a user's password, requiring them to change it. If a user tries to sign in after the API request, Amazon Cognito responds with a `PasswordResetRequiredException` error. Your app must then complete the forgot-password flow by prompting the user for their code and a new password, then submitting those values in a [ConfirmForgotPassword](#) request. In addition, if the user pool has phone verification selected and a verified phone number exists for the user, or if email verification is selected and a verified email exists for the user, calling this API will also result in sending a message to the end user with the code to change their password.

To use this API operation, your user pool must have self-service account recovery configured.

Use [AdminSetUserPassword](#) if you manage passwords as an administrator.

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "ClientMetadata": {  
    "string" : "string"  
  },  
  "Username": "string",  
  "UserPoolId": "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.

[ClientMetadata](#)

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If `username` isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to reset the user's password.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example resets the password for the user "testuser" and passes a `ClientMetadata` object to Lambda trigger events that can take a `ForgotPassword` trigger source.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminResetUserPassword
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser",
  "ClientMetadata": {
    "MyTestKey": "MyTestValue"
  }
}
```


Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

AdminRespondToAuthChallenge

Some API operations in a user pool generate a challenge, like a prompt for an MFA code, for device authentication that bypasses MFA, or for a custom authentication challenge. An `AdminRespondToAuthChallenge` API request provides the answer to that challenge, like a code or a secure remote password (SRP). The parameters of a response to an authentication challenge vary with the type of challenge.

For more information about custom authentication challenges, see [Custom authentication challenge Lambda triggers](#).

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "AnalyticsMetadata": {
    "AnalyticsEndpointId": "string"
  },
  "ChallengeName": "string",
  "ChallengeResponses": {
    "string" : "string"
  },
  "ClientId": "string",
  "ClientMetadata": {
    "string" : "string"
  },
  "ContextData": {
    "EncodedData": "string",
    "HttpHeaders": [
      {
        "headerName": "string",
        "headerValue": "string"
      }
    ],
    "IpAddress": "string",
    "ServerName": "string",
    "ServerPath": "string"
  },
  "Session": "string",
  "UserPoolId": "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.

[AnalyticsMetadata](#)

Information that supports analytics outcomes with Amazon Pinpoint, including the user's endpoint ID. The endpoint ID is a destination for Amazon Pinpoint push notifications, for example a device identifier, email address, or phone number.

Type: [AnalyticsMetadataType](#) object

Required: No

ChallengeName

The name of the challenge that you are responding to.

Possible challenges include the following:

Note

All of the following challenges require USERNAME and, when the app client has a client secret, SECRET_HASH in the parameters. Include a DEVICE_KEY for device authentication.

- **WEB_AUTHN**: Respond to the challenge with the results of a successful authentication with a WebAuthn authenticator, or passkey, as CREDENTIAL. Examples of WebAuthn authenticators include biometric devices and security keys.
- **PASSWORD**: Respond with the user's password as PASSWORD.
- **PASSWORD_SRP**: Respond with the initial SRP secret as SRP_A.
- **SELECT_CHALLENGE**: Respond with a challenge selection as ANSWER. It must be one of the challenge types in the AvailableChallenges response parameter. Add the parameters of the selected challenge, for example USERNAME and SMS_OTP.
- **SMS_MFA**: Respond with the code that your user pool delivered in an SMS message, as SMS_MFA_CODE
- **EMAIL_MFA**: Respond with the code that your user pool delivered in an email message, as EMAIL_MFA_CODE
- **EMAIL_OTP**: Respond with the code that your user pool delivered in an email message, as EMAIL_OTP_CODE .
- **SMS_OTP**: Respond with the code that your user pool delivered in an SMS message, as SMS_OTP_CODE.
- **PASSWORD_VERIFIER**: Respond with the second stage of SRP secrets as PASSWORD_CLAIM_SIGNATURE, PASSWORD_CLAIM_SECRET_BLOCK, and TIMESTAMP.
- **CUSTOM_CHALLENGE**: This is returned if your custom authentication flow determines that the user should pass another challenge before tokens are issued. The parameters of the challenge

are determined by your Lambda function and issued in the `ChallengeParameters` of a challenge response.

- `DEVICE_SRP_AUTH`: Respond with the initial parameters of device SRP authentication. For more information, see [Signing in with a device](#).
- `DEVICE_PASSWORD_VERIFIER`: Respond with `PASSWORD_CLAIM_SIGNATURE`, `PASSWORD_CLAIM_SECRET_BLOCK`, and `TIMESTAMP` after client-side SRP calculations. For more information, see [Signing in with a device](#).
- `NEW_PASSWORD_REQUIRED`: For users who are required to change their passwords after successful first login. Respond to this challenge with `NEW_PASSWORD` and any required attributes that Amazon Cognito returned in the `requiredAttributes` parameter. You can also set values for attributes that aren't required by your user pool and that your app client can write.

Amazon Cognito only returns this challenge for users who have temporary passwords. When you create passwordless users, you must provide values for all required attributes.

 Note

In a `NEW_PASSWORD_REQUIRED` challenge response, you can't modify a required attribute that already has a value. In `AdminRespondToAuthChallenge` or `RespondToAuthChallenge`, set a value for any keys that Amazon Cognito returned in the `requiredAttributes` parameter, then use the `AdminUpdateUserAttributes` or `UpdateUserAttributes` API operation to modify the value of any additional attributes.

- `MFA_SETUP`: For users who are required to setup an MFA factor before they can sign in. The MFA types activated for the user pool will be listed in the challenge parameters `MFAS_CAN_SETUP` value.

To set up time-based one-time password (TOTP) MFA, use the session returned in this challenge from `InitiateAuth` or `AdminInitiateAuth` as an input to `AssociateSoftwareToken`. Then, use the session returned by `VerifySoftwareToken` as an input to `RespondToAuthChallenge` or `AdminRespondToAuthChallenge` with challenge name `MFA_SETUP` to complete sign-in.

To set up SMS or email MFA, collect a `phone_number` or `email` attribute for the user. Then restart the authentication flow with an `InitiateAuth` or `AdminInitiateAuth` request.

Type: String

Valid Values: SMS_MFA | EMAIL_OTP | SOFTWARE_TOKEN_MFA | SELECT_MFA_TYPE | MFA_SETUP | PASSWORD_VERIFIER | CUSTOM_CHALLENGE | SELECT_CHALLENGE | DEVICE_SRP_AUTH | DEVICE_PASSWORD_VERIFIER | ADMIN_NO_SRP_AUTH | NEW_PASSWORD_REQUIRED | SMS_OTP | PASSWORD | WEB_AUTHN | PASSWORD_SRP

Required: Yes

ChallengeResponses

The responses to the challenge that you received in the previous request. Each challenge has its own required response parameters. The following examples are partial JSON request bodies that highlight challenge-response parameters.

Important

You must provide a SECRET_HASH parameter in all challenge responses to an app client that has a client secret. Include a DEVICE_KEY for device authentication.

SELECT_CHALLENGE

```
"ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses":  
{ "USERNAME": "[username]", "ANSWER": "[Challenge name]"}
```

Available challenges are PASSWORD, PASSWORD_SRP, EMAIL_OTP, SMS_OTP, and WEB_AUTHN.

Complete authentication in the SELECT_CHALLENGE response for PASSWORD, PASSWORD_SRP, and WEB_AUTHN:

- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses":
{ "ANSWER": "WEB_AUTHN", "USERNAME": "[username]", "CREDENTIAL":
"[AuthenticationResponseJSON]"}

See [AuthenticationResponseJSON](#).

- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses":
{ "ANSWER": "PASSWORD", "USERNAME": "[username]", "PASSWORD":
"[password]"}

- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses":
 { "ANSWER": "PASSWORD_SRP", "USERNAME": "[username]", "SRP_A":
 "[SRP_A]"}

For SMS_OTP and EMAIL_OTP, respond with the username and answer. Your user pool will send a code for the user to submit in the next challenge response.

- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses":
 { "ANSWER": "SMS_OTP", "USERNAME": "[username]"}
- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses":
 { "ANSWER": "EMAIL_OTP", "USERNAME": "[username]"}

WEB_AUTHN

```
"ChallengeName": "WEB_AUTHN", "ChallengeResponses": { "USERNAME":  
"[username]", "CREDENTIAL": "[AuthenticationResponseJSON]"}
```

See [AuthenticationResponseJSON](#).

PASSWORD

```
"ChallengeName": "PASSWORD", "ChallengeResponses": { "USERNAME":  
"[username]", "PASSWORD": "[password]"}
```

PASSWORD_SRP

```
"ChallengeName": "PASSWORD_SRP", "ChallengeResponses": { "USERNAME":  
"[username]", "SRP_A": "[SRP_A]"}
```

SMS_OTP

```
"ChallengeName": "SMS_OTP", "ChallengeResponses": {"SMS_OTP_CODE":  
"[code]", "USERNAME": "[username]"}
```

EMAIL_OTP

```
"ChallengeName": "EMAIL_OTP", "ChallengeResponses": {"EMAIL_OTP_CODE":  
"[code]", "USERNAME": "[username]"}
```

SMS_MFA

```
"ChallengeName": "SMS_MFA", "ChallengeResponses": {"SMS_MFA_CODE":  
"[code]", "USERNAME": "[username]"}
```

PASSWORD_VERIFIER

This challenge response is part of the SRP flow. Amazon Cognito requires that your application respond to this challenge within a few seconds. When the response time exceeds this period, your user pool returns a `NotAuthorizedException` error.

```
"ChallengeName": "PASSWORD_VERIFIER", "ChallengeResponses":  
{  
  "PASSWORD_CLAIM_SIGNATURE": "[claim_signature]",  
  "PASSWORD_CLAIM_SECRET_BLOCK": "[secret_block]", "TIMESTAMP":  
  [timestamp], "USERNAME": "[username]"}
```

CUSTOM_CHALLENGE

```
"ChallengeName": "CUSTOM_CHALLENGE", "ChallengeResponses":  
{  
  "USERNAME": "[username]", "ANSWER": "[challenge_answer]"}
```

NEW_PASSWORD_REQUIRED

```
"ChallengeName": "NEW_PASSWORD_REQUIRED", "ChallengeResponses":  
{  
  "NEW_PASSWORD": "[new_password]", "USERNAME": "[username]"}
```

To set any required attributes that `InitiateAuth` returned in an `requiredAttributes` parameter, add `"userAttributes.[attribute_name]": "[attribute_value]"`. This parameter can also set values for writable attributes that aren't required by your user pool.

Note

In a `NEW_PASSWORD_REQUIRED` challenge response, you can't modify a required attribute that already has a value. In `AdminRespondToAuthChallenge` or `RespondToAuthChallenge`, set a value for any keys that Amazon Cognito returned in the `requiredAttributes` parameter, then use the `AdminUpdateUserAttributes` or `UpdateUserAttributes` API operation to modify the value of any additional attributes.

SOFTWARE_TOKEN_MFA

```
"ChallengeName": "SOFTWARE_TOKEN_MFA", "ChallengeResponses":  
{  
  "USERNAME": "[username]", "SOFTWARE_TOKEN_MFA_CODE":  
  [authenticator_code]}
```


DEVICE_SRP_AUTH

```
"ChallengeName": "DEVICE_SRP_AUTH", "ChallengeResponses": {"USERNAME": "[username]", "DEVICE_KEY": "[device_key]", "SRP_A": "[srp_a]"}
```

DEVICE_PASSWORD_VERIFIER

```
"ChallengeName": "DEVICE_PASSWORD_VERIFIER", "ChallengeResponses": {"DEVICE_KEY": "[device_key]", "PASSWORD_CLAIM_SIGNATURE": "[claim_signature]", "PASSWORD_CLAIM_SECRET_BLOCK": "[secret_block]", "TIMESTAMP": [timestamp], "USERNAME": "[username]"}
```

MFA_SETUP

```
"ChallengeName": "MFA_SETUP", "ChallengeResponses": {"USERNAME": "[username]"}, "SESSION": "[Session ID from VerifySoftwareToken]"
```

SELECT_MFA_TYPE

```
"ChallengeName": "SELECT_MFA_TYPE", "ChallengeResponses": {"USERNAME": "[username]", "ANSWER": "[SMS_MFA|EMAIL_MFA|SOFTWARE_TOKEN_MFA]"}
```

For more information about SECRET_HASH, see [Computing secret hash values](#). For information about DEVICE_KEY, see [Working with user devices in your user pool](#).

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ClientId

The ID of the app client where you initiated sign-in.

Type: String

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

Pattern: `[\w+]`

Required: Yes

ClientMetadata

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ContextData

Contextual data about your user session like the device fingerprint, IP address, or location. Amazon Cognito threat protection evaluates the risk of an authentication event based on the context that your app generates and passes to Amazon Cognito when it makes API requests.

For more information, see [Collecting data for threat protection in applications](#).

Type: [ContextDataType](#) object

Required: No

Session

The session identifier that maintains the state of authentication requests and challenge responses. If an `AdminInitiateAuth` or `AdminRespondToAuthChallenge` API request results in a determination that your application must pass another challenge, Amazon Cognito returns a session with other challenge parameters. Send this session identifier, unmodified, to the next `AdminRespondToAuthChallenge` request.

Type: String

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

Required: No

UserPoolId

The ID of the user pool where you want to respond to an authentication challenge.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "AuthenticationResult": {
    "AccessToken": "string",
    "ExpiresIn": number,
```

```
"IdToken": "string",
"NewDeviceMetadata": {
  "DeviceGroupKey": "string",
  "DeviceKey": "string"
},
"RefreshToken": "string",
"TokenType": "string"
},
"ChallengeName": "string",
"ChallengeParameters": {
  "string" : "string"
},
"Session": "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.

AuthenticationResult

The outcome of a successful authentication process. After your application has passed all challenges, Amazon Cognito returns an `AuthenticationResult` with the JSON web tokens (JWTs) that indicate successful sign-in.

Type: [AuthenticationResultType](#) object

ChallengeName

The name of the next challenge that you must respond to.

Possible challenges include the following:

Note

All of the following challenges require USERNAME and, when the app client has a client secret, SECRET_HASH in the parameters. Include a DEVICE_KEY for device authentication.

- **WEB_AUTHN**: Respond to the challenge with the results of a successful authentication with a WebAuthn authenticator, or passkey, as CREDENTIAL. Examples of WebAuthn authenticators include biometric devices and security keys.
- **PASSWORD**: Respond with the user's password as PASSWORD.
- **PASSWORD_SRP**: Respond with the initial SRP secret as SRP_A.
- **SELECT_CHALLENGE**: Respond with a challenge selection as ANSWER. It must be one of the challenge types in the AvailableChallenges response parameter. Add the parameters of the selected challenge, for example USERNAME and SMS_OTP.
- **SMS_MFA**: Respond with the code that your user pool delivered in an SMS message, as SMS_MFA_CODE
- **EMAIL_MFA**: Respond with the code that your user pool delivered in an email message, as EMAIL_MFA_CODE
- **EMAIL_OTP**: Respond with the code that your user pool delivered in an email message, as EMAIL_OTP_CODE .
- **SMS_OTP**: Respond with the code that your user pool delivered in an SMS message, as SMS_OTP_CODE.
- **PASSWORD_VERIFIER**: Respond with the second stage of SRP secrets as PASSWORD_CLAIM_SIGNATURE, PASSWORD_CLAIM_SECRET_BLOCK, and TIMESTAMP.
- **CUSTOM_CHALLENGE**: This is returned if your custom authentication flow determines that the user should pass another challenge before tokens are issued. The parameters of the challenge are determined by your Lambda function and issued in the ChallengeParameters of a challenge response.
- **DEVICE_SRP_AUTH**: Respond with the initial parameters of device SRP authentication. For more information, see [Signing in with a device](#).
- **DEVICE_PASSWORD_VERIFIER**: Respond with PASSWORD_CLAIM_SIGNATURE, PASSWORD_CLAIM_SECRET_BLOCK, and TIMESTAMP after client-side SRP calculations. For more information, see [Signing in with a device](#).
- **NEW_PASSWORD_REQUIRED**: For users who are required to change their passwords after successful first login. Respond to this challenge with NEW_PASSWORD and any required attributes that Amazon Cognito returned in the requiredAttributes parameter. You can also set values for attributes that aren't required by your user pool and that your app client can write.

Amazon Cognito only returns this challenge for users who have temporary passwords. When you create passwordless users, you must provide values for all required attributes.

 Note

In a `NEW_PASSWORD_REQUIRED` challenge response, you can't modify a required attribute that already has a value. In `AdminRespondToAuthChallenge` or `RespondToAuthChallenge`, set a value for any keys that Amazon Cognito returned in the `requiredAttributes` parameter, then use the `AdminUpdateUserAttributes` or `UpdateUserAttributes` API operation to modify the value of any additional attributes.

- `MFA_SETUP`: For users who are required to setup an MFA factor before they can sign in. The MFA types activated for the user pool will be listed in the challenge parameters `MFAS_CAN_SETUP` value.

To set up time-based one-time password (TOTP) MFA, use the session returned in this challenge from `InitiateAuth` or `AdminInitiateAuth` as an input to `AssociateSoftwareToken`. Then, use the session returned by `VerifySoftwareToken` as an input to `RespondToAuthChallenge` or `AdminRespondToAuthChallenge` with challenge name `MFA_SETUP` to complete sign-in.

To set up SMS or email MFA, collect a `phone_number` or `email` attribute for the user. Then restart the authentication flow with an `InitiateAuth` or `AdminInitiateAuth` request.

Type: String

Valid Values: `SMS_MFA` | `EMAIL_OTP` | `SOFTWARE_TOKEN_MFA` | `SELECT_MFA_TYPE` | `MFA_SETUP` | `PASSWORD_VERIFIER` | `CUSTOM_CHALLENGE` | `SELECT_CHALLENGE` | `DEVICE_SRP_AUTH` | `DEVICE_PASSWORD_VERIFIER` | `ADMIN_NO_SRP_AUTH` | `NEW_PASSWORD_REQUIRED` | `SMS_OTP` | `PASSWORD` | `WEB_AUTHN` | `PASSWORD_SRP`

ChallengeParameters

The parameters that define your response to the next challenge.

Take the values in `ChallengeParameters` and provide values for them in the `ChallengeResponses` of the next [AdminRespondToAuthChallenge](#) request.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Session

The session identifier that maintains the state of authentication requests and challenge responses. If an `AdminInitiateAuth` or `AdminRespondToAuthChallenge` API request results in a determination that your application must pass another challenge, Amazon Cognito returns a session with other challenge parameters. Send this session identifier, unmodified, to the next `AdminRespondToAuthChallenge` request.

Type: String

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

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AliasExistsException

This exception is thrown when a user tries to confirm the account with an email address or phone number that has already been supplied as an alias for a different user profile. This exception indicates that an account with this email address or phone already exists in a user pool that you've configured to use email address or phone number as a sign-in alias.

message

The message that Amazon Cognito sends to the user when the value of an alias attribute is already linked to another user profile.

HTTP Status Code: 400

CodeMismatchException

This exception is thrown if the provided code doesn't match what the server was expecting.

message

The message provided when the code mismatch exception is thrown.

HTTP Status Code: 400

ExpiredCodeException

This exception is thrown if a code has expired.

message

The message returned when the expired code exception is thrown.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidPasswordException

This exception is thrown when Amazon Cognito encounters an invalid password.

message

The message returned when Amazon Cognito throws an invalid user password exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

MFAMethodNotFoundException

This exception is thrown when Amazon Cognito can't find a multi-factor authentication (MFA) method.

message

The message returned when Amazon Cognito throws an MFA method not found exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordHistoryPolicyViolationException

The message returned when a user's new password matches a previous password and doesn't comply with the password-history policy.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

SoftwareTokenMFANotFoundException

This exception is thrown when the software token time-based one-time password (TOTP) multi-factor authentication (MFA) isn't activated for the user pool.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example provides an authenticator-app password in response to a TOTP challenge.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminRespondToAuthChallenge
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ChallengeName": "SOFTWARE_TOKEN_MFA",
  "ClientId": "1example23456789",
  "UserPoolId": "us-west-2_EXAMPLE",
  "ChallengeResponses": {
    "USERNAME": "testuser",
    "SOFTWARE_TOKEN_MFA_CODE": "123456",
```

```
"SECRET_HASH": "cKtx2L2fvV1FeAbk3iUPgCyXY+5B0It00ItxhFaLkeA="
},
"Session": "EXAMPLE_SESSION_TOKEN_FROM_ADMININITIATEAUTH..."
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "AuthenticationResult": {
    "AccessToken": "eyJraACCESSEXAMPLE...",
    "ExpiresIn": 3600,
    "IdToken": "eyJraIDEXAMPLE...",
    "NewDeviceMetadata": {
      "DeviceGroupKey": "-v7w9UcY6",
      "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
    "RefreshToken": "eyJjREFRESHEXAMPLE...",
    "TokenType": "Bearer"
  },
  "ChallengeParameters": {}
}
```

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](#)

AdminSetUserMFAPreference

Sets the user's multi-factor authentication (MFA) preference, including which MFA options are activated, and if any are preferred. Only one factor can be set as preferred. The preferred MFA factor will be used to authenticate a user if multiple factors are activated. If multiple options are activated and no preference is set, a challenge to choose an MFA option will be returned during sign-in.

This operation doesn't reset an existing TOTP MFA for a user. To register a new TOTP factor for a user, make an [AssociateSoftwareToken](#) request. For more information, see [TOTP software token MFA](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "EmailMfaSettings": {
    "Enabled": boolean,
    "PreferredMfa": boolean
  },
  "SMSMfaSettings": {
    "Enabled": boolean,
    "PreferredMfa": boolean
  },
  "SoftwareTokenMfaSettings": {
    "Enabled": boolean,
    "PreferredMfa": boolean
  },
  "Username": "string",
```

```
"UserPoolId": "string",  
"WebAuthnMfaSettings": {  
  "Enabled": boolean  
}  
}
```

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.

[EmailMfaSettings](#)

User preferences for email message MFA. Activates or deactivates email MFA and sets it as the preferred MFA method when multiple methods are available. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

Type: [EmailMfaSettingsType](#) object

Required: No

[SMSMfaSettings](#)

User preferences for SMS message MFA. Activates or deactivates SMS MFA and sets it as the preferred MFA method when multiple methods are available.

Type: [SMSMfaSettingsType](#) object

Required: No

[SoftwareTokenMfaSettings](#)

User preferences for time-based one-time password (TOTP) MFA. Activates or deactivates TOTP MFA and sets it as the preferred MFA method when multiple methods are available.

Type: [SoftwareTokenMfaSettingsType](#) object

Required: No

[Username](#)

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If `username` isn't an alias

attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to set a user's MFA preferences.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

WebAuthnMfaSettings

User preferences for passkey MFA. Activates or deactivates passkey MFA for the user. When activated, passkey authentication requires user verification, and passkey sign-in is available when MFA is required. To activate this setting, the `FactorConfiguration` of your user pool `WebAuthnConfiguration` must be `MULTI_FACTOR_WITH_USER_VERIFICATION`. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

Type: [WebAuthnMfaSettingsType](#) 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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request sets the user "testuser" to have both SMS and TOTP sign-in available, but to prefer SMS messages.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminSetUserMFAPreference
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
```

```
{
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser",
  "SMSMfaSettings": {
    "Enabled": true,
    "PreferredMfa": true
  },
  "SoftwareTokenMfaSettings": {
    "Enabled": true,
    "PreferredMfa": false
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

AdminSetUserPassword

Sets the specified user's password in a user pool. This operation administratively sets a temporary or permanent password for a user. With this operation, you can bypass self-service password changes and permit immediate sign-in with the password that you set. To do this, set `Permanent` to `true`.

You can also set a new temporary password in this request, send it to a user, and require them to choose a new password on their next sign-in. To do this, set `Permanent` to `false`.

If the password is temporary, the user's `Status` becomes `FORCE_CHANGE_PASSWORD`. When the user next tries to sign in, the `InitiateAuth` or `AdminInitiateAuth` response includes the `NEW_PASSWORD_REQUIRED` challenge. If the user doesn't sign in before the temporary password expires, they can no longer sign in and you must repeat this operation to set a temporary or permanent password for them.

After the user sets a new password, or if you set a permanent password, their status becomes `Confirmed`.

`AdminSetUserPassword` can set a password for the user profile that Amazon Cognito creates for third-party federated users. When you set a password, the federated user's status changes from `EXTERNAL_PROVIDER` to `CONFIRMED`. A user in this state can sign in as a federated user, and initiate authentication flows in the API like a linked native user. They can also modify their password and attributes in token-authenticated API requests like `ChangePassword` and `UpdateUserAttributes`. As a best security practice and to keep users in sync with your external IdP, don't set passwords on federated user profiles. To set up a federated user for native sign-in with a linked native user, refer to [Linking federated users to an existing user profile](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "Password": "string",  
  "Permanent": boolean,  
  "Username": "string",  
  "UserPoolId": "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.

Password

The new temporary or permanent password that you want to set for the user. You can't remove the password for a user who already has a password so that they can only sign in with passwordless methods. In this scenario, you must create a new user without a password.

Type: String

Length Constraints: Maximum length of 256.

Pattern: `[\S]+`

Required: Yes

Permanent

Set to `true` to set a password that the user can immediately sign in with. Set to `false` to set a temporary password that the user must change on their next sign-in.

Type: Boolean

Required: No

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If `username` isn't an alias

attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to set the user's password.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidPasswordException

This exception is thrown when Amazon Cognito encounters an invalid password.

message

The message returned when Amazon Cognito throws an invalid user password exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordHistoryPolicyViolationException

The message returned when a user's new password matches a previous password and doesn't comply with the password-history policy.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request sets the user "testuser" to have the password "MyExamplePassword1=", and to be able to sign in with that password without a reset.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminSetUserPassword
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "Password": "MyExamplePassword1=",
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser",
  "Permanent": true
}
```

```
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

AdminSetUserSettings

This action is no longer supported. You can use it to configure only SMS MFA. You can't use it to configure time-based one-time password (TOTP) software token MFA.

To configure all types of MFA, use [AdminSetUserMFAPreference](#) instead.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "MFAOptions": [  
    {  
      "AttributeName": "string",  
      "DeliveryMedium": "string"  
    }  
  ],  
  "Username": "string",  
  "UserPoolId": "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.

MFAOptions

You can use this parameter only to set an SMS configuration that uses SMS for delivery.

Type: Array of [MFAMOptionType](#) objects

Required: Yes

[Username](#)

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

[UserPoolId](#)

The ID of the user pool that contains the user whose options you're setting.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

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](#)

AdminUpdateAuthEventFeedback

Provides the feedback for an authentication event generated by threat protection features. Your response indicates that you think that the event either was from a valid user or was an unwanted authentication attempt. This feedback improves the risk evaluation decision for the user pool as part of Amazon Cognito threat protection. To activate this setting, your user pool must be on the [Plus tier](#).

To train the threat-protection model to recognize trusted and untrusted sign-in characteristics, configure threat protection in audit-only mode and provide a mechanism for users or administrators to submit feedback. Your feedback can tell Amazon Cognito that a risk rating was assigned at a level you don't agree with.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "EventId": "string",  
  "FeedbackValue": "string",  
  "Username": "string",  
  "UserPoolId": "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.

EventId

The ID of the threat protection authentication event that you want to update.

To query authentication events for a user, see [AdminListUserAuthEvents](#).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 50.

Pattern: `[\w+-]+`

Required: Yes

FeedbackValue

Your feedback to the authentication event. When you provide a `FeedbackValue` value of `valid`, you tell Amazon Cognito that you trust a user session where Amazon Cognito has evaluated some level of risk. When you provide a `FeedbackValue` value of `invalid`, you tell Amazon Cognito that you don't trust a user session, or you don't believe that Amazon Cognito evaluated a high-enough risk level.

Type: String

Valid Values: `Valid` | `Invalid`

Required: Yes

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If `username` isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to submit authentication-event feedback.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

UserPoolAddOnNotEnabledException

This exception is thrown when user pool add-ons aren't enabled.

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](#)

AdminUpdateDeviceStatus

Updates the status of a user's device so that it is marked as remembered or not remembered for the purpose of device authentication. Device authentication is a "remember me" mechanism that silently completes sign-in from trusted devices with a device key instead of a user-provided MFA code. This operation changes the status of a device without deleting it, so you can enable it again later. For more information about device authentication, see [Working with devices](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "DeviceKey": "string",
  "DeviceRememberedStatus": "string",
  "Username": "string",
  "UserPoolId": "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.

DeviceKey

The unique identifier, or device key, of the device that you want to update the status for.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-f-]+`

Required: Yes

DeviceRememberedStatus

To enable device authentication with the specified device, set to `remembered`. To disable, set to `not_remembered`.

Type: String

Valid Values: `remembered` | `not_remembered`

Required: No

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If `username` isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to change a user's device status.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request sets the device with key "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" to be remembered for device authentication in future sign-in attempts.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminUpdateDeviceStatus
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser",
  "DeviceRememberedStatus": "remembered"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

AdminUpdateUserAttributes

Updates the specified user's attributes. To delete an attribute from your user, submit the attribute in your API request with a blank value.

For custom attributes, you must add a `custom:` prefix to the attribute name, for example `custom:department`.

This operation can set a user's email address or phone number as verified and permit immediate sign-in in user pools that require verification of these attributes. To do this, set the `email_verified` or `phone_number_verified` attribute to `true`.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Request Syntax

```
{
  "ClientMetadata": {
    "string" : "string"
  },
  "UserAttributes": [
    {
      "Name": "string",
      "Value": "string"
    }
  ],
  "Username": "string",
  "UserPoolId": "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.

ClientMetadata

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

UserAttributes

An array of name-value pairs representing user attributes.

For custom attributes, you must prepend the `custom:` prefix to the attribute name.

If your user pool requires verification before Amazon Cognito updates an attribute value that you specify in this request, Amazon Cognito doesn't immediately update the value of that attribute. After your user receives and responds to a verification message to verify the new value, Amazon Cognito updates the attribute value. Your user can sign in and receive messages with the original attribute value until they verify the new value.

To skip the verification message and update the value of an attribute that requires verification in the same API request, include the `email_verified` or `phone_number_verified` attribute, with a value of `true`. If you set the `email_verified` or `phone_number_verified` value for an `email` or `phone_number` attribute that requires verification to `true`, Amazon Cognito doesn't send a verification message to your user.

Type: Array of [AttributeType](#) objects

Required: Yes

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to update user attributes.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

AliasExistsException

This exception is thrown when a user tries to confirm the account with an email address or phone number that has already been supplied as an alias for a different user profile. This exception indicates that an account with this email address or phone already exists in a user pool that you've configured to use email address or phone number as a sign-in alias.

message

The message that Amazon Cognito sends to the user when the value of an alias attribute is already linked to another user profile.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request sets the values of two attributes for "testuser." The request also includes client metadata that the user pool passes on in a CustomMessage_UpdateUserAttribute Lambda trigger event.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminUpdateUserAttributes
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "UserAttributes": [
    {
      "Name": "custom:deliverables",
      "Value": "project-111222"
    },
    {
      "Name": "name",
      "Value": "John"
    }
  ],
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser",
  "ClientMetadata": {
    "MyTestKey": "MyTestValue"
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
```

```
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{}
```

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](#)

AdminUserGlobalSignOut

Invalidates the identity, access, and refresh tokens that Amazon Cognito issued to a user. Call this operation with your administrative credentials when your user signs out of your app. This results in the following behavior.

- Amazon Cognito no longer accepts *token-authorized* user operations that you authorize with a signed-out user's access tokens. For more information, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Amazon Cognito returns an `Access Token has been revoked` error when your app attempts to authorize a user pools API request with a revoked access token that contains the scope `aws.cognito.signin.user.admin`.

- Amazon Cognito no longer accepts a signed-out user's ID token in a [GetId](#) request to an identity pool with `ServerSideTokenCheck` enabled for its user pool IdP configuration in [CognitoIdentityProvider](#).
- Amazon Cognito no longer accepts a signed-out user's refresh tokens in refresh requests.

Other requests might be valid until your user's token expires. This operation doesn't clear the [managed login](#) session cookie. To clear the session for a user who signed in with managed login or the classic hosted UI, direct their browser session to the [logout endpoint](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
```

```
"Username": "string",  
"UserPoolId": "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.

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If `username` isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to sign out a user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request signs out the user "testuser."

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AdminUserGlobalSignOut
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE",
  "Username": "testuser",
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

AssociateSoftwareToken

Begins setup of time-based one-time password (TOTP) multi-factor authentication (MFA) for a user, with a unique private key that Amazon Cognito generates and returns in the API response. You can authorize an AssociateSoftwareToken request with either the user's access token, or a session string from a challenge response that you received from Amazon Cognito.

Note

Amazon Cognito disassociates an existing software token when you verify the new token in a [VerifySoftwareToken](#) API request. If you don't verify the software token and your user pool doesn't require MFA, the user can then authenticate with user name and password credentials alone. If your user pool requires TOTP MFA, Amazon Cognito generates an MFA_SETUP or SOFTWARE_TOKEN_SETUP challenge each time your user signs in. Complete setup with AssociateSoftwareToken and VerifySoftwareToken. After you set up software token MFA for your user, Amazon Cognito generates a SOFTWARE_TOKEN_MFA challenge when they authenticate. Respond to this challenge with your user's TOTP.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Request Syntax

```
{  
  "AccessToken": "string",  
  "Session": "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.

AccessToken

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws:cognito.signin.user.admin`.

You can provide either an access token or a session ID in the request.

Type: String

Pattern: `[A-Za-z0-9-_=.]`+

Required: No

Session

The session identifier that maintains the state of authentication requests and challenge responses. In `AssociateSoftwareToken`, this is the session ID from a successful sign-in. You can provide either an access token or a session ID in the request.

Type: String

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

Required: No

Response Syntax

```
{
  "SecretCode": "string",
  "Session": "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.

SecretCode

A unique generated shared secret code that is used by the TOTP algorithm to generate a one-time code.

Type: String

Length Constraints: Minimum length of 16.

Pattern: [A-Za-z0-9]+

Session

The session identifier that maintains the state of authentication requests and challenge responses.

This session ID is valid for the next request in this flow, [VerifySoftwareToken](#).

Type: String

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

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

SoftwareTokenMFANotFoundException

This exception is thrown when the software token time-based one-time password (TOTP) multi-factor authentication (MFA) isn't activated for the user pool.

HTTP Status Code: 400

Examples

Example

The following example request generates a TOTP private key for the user who the access key was issued to.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.AssociateSoftwareToken
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJraACCESSEXAMPLE..."
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "SecretCode": "PRIVATECODEEXAMPLE..."
}
```

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](#)

ChangePassword

Changes the password for the currently signed-in user.

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{  
  "AccessToken": "string",  
  "PreviousPassword": "string",  
  "ProposedPassword": "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.

AccessToken

A valid access token that Amazon Cognito issued to the user whose password you want to change.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: Yes

PreviousPassword

The user's previous password. Required if the user has a password. If the user has no password and only signs in with passwordless authentication options, you can omit this parameter.

Type: String

Length Constraints: Maximum length of 256.

Pattern: `[\S]+`

Required: No

ProposedPassword

A new password that you prompted the user to enter in your application.

Type: String

Length Constraints: Maximum length of 256.

Pattern: `[\S]+`

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](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidPasswordException

This exception is thrown when Amazon Cognito encounters an invalid password.

message

The message returned when Amazon Cognito throws an invalid user password exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordHistoryPolicyViolationException

The message returned when a user's new password matches a previous password and doesn't comply with the password-history policy.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example changes the password of the user with the access key "eyJra456defEXAMPLE" and current password "MyCurrentPassword1!".

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ChangePassword
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE",
  "PreviousPassword": "MyCurrentPassword1!",
  "ProposedPassword": "MyNewPassword2!"
}
```

Sample Response

```
HTTP/1.1 200 OK
```

```
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

CompleteWebAuthnRegistration

Completes registration of a passkey authenticator for the currently signed-in user.

Your application provides data from a successful registration request with the data from the output of a [StartWebAuthnRegistration](#).

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Request Syntax

```
{
  "AccessToken": "string",
  "Credential": JSON value
}
```

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.

[AccessToken](#)

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_=.]`+

Required: Yes

[Credential](#)

A [RegistrationResponseJSON](#) public-key credential response from the user's passkey provider.

Type: JSON value

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](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

WebAuthnChallengeNotFoundException

This exception is thrown when the challenge from StartWebAuthn registration has expired.

HTTP Status Code: 400

WebAuthnClientMismatchException

This exception is thrown when the access token is for a different client than the one in the original StartWebAuthnRegistration request.

HTTP Status Code: 400

WebAuthnCredentialNotSupportedException

This exception is thrown when a user presents passkey credentials from an unsupported device or provider.

HTTP Status Code: 400

WebAuthnNotEnabledException

This exception is thrown when the passkey feature isn't enabled for the user pool.

HTTP Status Code: 400

WebAuthnOriginNotAllowedException

This exception is thrown when the passkey credential's registration origin does not align with the user pool relying party id.

HTTP Status Code: 400

WebAuthnRelyingPartyMismatchException

This exception is thrown when the given passkey credential is associated with a different relying party ID than the user pool relying party ID.

HTTP Status Code: 400

Examples

Example

The following example completes passkey registration for the user with access token "eyJra456defEXAMPLE".

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.CompleteWebAuthnRegistration
User-Agent: <UserAgentString>
```



```
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE",
  "Credential": "[RegistrationResponseJSON]"
}
```

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](#)

ConfirmDevice

Confirms a device that a user wants to remember. A remembered device is a "Remember me on this device" option for user pools that perform authentication with the device key of a trusted device in the back end, instead of a user-provided MFA code. For more information about device authentication, see [Working with user devices in your user pool](#).

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{
  "AccessToken": "string",
  "DeviceKey": "string",
  "DeviceName": "string",
  "DeviceSecretVerifierConfig": {
    "PasswordVerifier": "string",
    "Salt": "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.

[AccessToken](#)

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws:cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_=.]`+

Required: Yes

[DeviceKey](#)

The unique identifier, or device key, of the device that you want to update the status for.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-f-]`+

Required: Yes

[DeviceName](#)

A friendly name for the device, for example `MyMobilePhone`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

[DeviceSecretVerifierConfig](#)

The configuration of the device secret verifier.

Type: [DeviceSecretVerifierConfigType](#) object

Required: No

Response Syntax

```
{
  "UserConfirmationNecessary": boolean
}
```

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.

UserConfirmationNecessary

When `true`, your user must confirm that they want to remember the device. Prompt the user for an answer.

You must then make an [UpdateDeviceStatus](#) request that sets the device to `remembered` or `not_remembered`.

When `false`, immediately sets the device as `remembered` and eligible for device authentication.

You can configure your user pool to always remember devices, in which case this response is `false`, or to allow users to opt in, in which case this response is `true`. Configure this option under *Device tracking* in the *Sign-in* menu of your user pool.

You can also configure this option with the `DeviceConfiguration` parameter of a [CreateUserPool](#) or [UpdateUserPool](#) request.

Type: Boolean

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

DeviceKeyExistsException

This exception is thrown when a user attempts to confirm a device with a device key that already exists.

HTTP Status Code: 400

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidPasswordException

This exception is thrown when Amazon Cognito encounters an invalid password.

message

The message returned when Amazon Cognito throws an invalid user password exception.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UsernameExistsException

This exception is thrown when Amazon Cognito encounters a user name that already exists in the user pool.

message

The message returned when Amazon Cognito throws a user name exists exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request confirms a device for the user with the access token "eyJra456defEXAMPLE". In the user pool in this example, the user must confirm that they want to remember the device with a new [UpdateDeviceStatus](#) request that sets

DeviceRememberedStatus to true for the device with key a1b2c3d4-5678-90ab-cdef-EXAMPLE11111.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ConfirmDevice
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE",
  "DeviceKey": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "DeviceName": "MyMobileDevice",
  "DeviceSecretVerifierConfig": {
    "PasswordVerifier": "[calculated verifier string]",
    "Salt": "[salt]"
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "UserConfirmationNecessary": true
}
```

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](#)

ConfirmForgotPassword

This public API operation accepts a confirmation code that Amazon Cognito sent to a user and accepts a new password for that user.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{
  "AnalyticsMetadata": {
    "AnalyticsEndpointId": "string"
  },
  "ClientId": "string",
  "ClientMetadata": {
    "string" : "string"
  },
  "ConfirmationCode": "string",
  "Password": "string",
  "SecretHash": "string",
  "UserContextData": {
    "EncodedData": "string",
    "IpAddress": "string"
  },
  "Username": "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.

AnalyticsMetadata

Information that supports analytics outcomes with Amazon Pinpoint, including the user's endpoint ID. The endpoint ID is a destination for Amazon Pinpoint push notifications, for example a device identifier, email address, or phone number.

Type: [AnalyticsMetadataType](#) object

Required: No

ClientId

The ID of the app client where the user wants to reset their password. This parameter is an identifier of the client application that users are resetting their password from, but this operation resets users' irrespective of the app clients they sign in to.

Type: String

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

Pattern: `[\w+]`

Required: Yes

ClientMetadata

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ConfirmationCode

The confirmation code that your user pool delivered when your user requested to reset their password.

Your user pool sends these codes in response to [AdminResetUserPassword](#) or [ForgotPassword](#) requests.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[\S]+`

Required: Yes

Password

The new password that your user wants to set.

Type: String

Length Constraints: Maximum length of 256.

Pattern: `[\S]+`

Required: Yes

SecretHash

A keyed-hash message authentication code (HMAC) calculated using the secret key of a user pool client and username plus the client ID in the message. For more information about SecretHash, see [Computing secret hash values](#).

Type: String

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

Pattern: `[\w+=/]+`

Required: No

UserContextData

Contextual data about your user session like the device fingerprint, IP address, or location. Amazon Cognito threat protection evaluates the risk of an authentication event based on the context that your app generates and passes to Amazon Cognito when it makes API requests.

For more information, see [Collecting data for threat protection in applications](#).

Type: [UserContextDataType](#) object

Required: No

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

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](#).

CodeMismatchException

This exception is thrown if the provided code doesn't match what the server was expecting.

message

The message provided when the code mismatch exception is thrown.

HTTP Status Code: 400

ExpiredCodeException

This exception is thrown if a code has expired.

message

The message returned when the expired code exception is thrown.

HTTP Status Code: 400

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidPasswordException

This exception is thrown when Amazon Cognito encounters an invalid password.

message

The message returned when Amazon Cognito throws an invalid user password exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordHistoryPolicyViolationException

The message returned when a user's new password matches a previous password and doesn't comply with the password-history policy.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyFailedAttemptsException

This exception is thrown when the user has made too many failed attempts for a given action, such as sign-in.

message

The message returned when Amazon Cognito returns a TooManyFailedAttempts exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request sets a new password for the user "testuser".

Sample Request

```
POST HTTP/1.1
```

```
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ConfirmForgotPassword
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ClientId": "lexample23456789",
  "ConfirmationCode": "123456",
  "Password": "MyNewPassword1!",
  "Username": "testuser"
}
```

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](#)

ConfirmSignUp

Confirms the account of a new user. This public API operation submits a code that Amazon Cognito sent to your user when they signed up in your user pool. After your user enters their code, they confirm ownership of the email address or phone number that they provided, and their user account becomes active. Depending on your user pool configuration, your users will receive their confirmation code in an email or SMS message.

Local users who signed up in your user pool are the only type of user who can confirm sign-up with a code. Users who federate through an external identity provider (IdP) have already been confirmed by their IdP.

Administrator-created users, users created with the [AdminCreateUser](#) API operation, confirm their accounts when they respond to their invitation email message and choose a password. They do not receive a confirmation code. Instead, they receive a temporary password.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{
  "AnalyticsMetadata": {
    "AnalyticsEndpointId": "string"
  },
  "ClientId": "string",
  "ClientMetadata": {
    "string" : "string"
  },
  "ConfirmationCode": "string",
  "ForceAliasCreation": boolean,
  "SecretHash": "string",
  "Session": "string",
```

```
"UserContextData": {  
  "EncodedData": "string",  
  "IpAddress": "string"  
},  
"Username": "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.

[AnalyticsMetadata](#)

Information that supports analytics outcomes with Amazon Pinpoint, including the user's endpoint ID. The endpoint ID is a destination for Amazon Pinpoint push notifications, for example a device identifier, email address, or phone number.

Type: [AnalyticsMetadataType](#) object

Required: No

[ClientId](#)

The ID of the app client associated with the user pool.

Type: String

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

Pattern: `[\w+]`

Required: Yes

[ClientMetadata](#)

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides

the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

 Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ConfirmationCode

The confirmation code that your user pool sent in response to the `SignUp` request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[\S]+`

Required: Yes

ForceAliasCreation

When `true`, forces user confirmation despite any existing aliases. Defaults to `false`. A value of `true` migrates the alias from an existing user to the new user if an existing user already has the phone number or email address as an alias.

Say, for example, that an existing user has an `email` attribute of `bob@example.com` and `email` is an alias in your user pool. If the new user also has an `email` of `bob@example.com` and your `ConfirmSignUp` response sets `ForceAliasCreation` to `true`, the new user can sign in with a username of `bob@example.com` and the existing user can no longer do so.

If `false` and an attribute belongs to an existing alias, this request returns an **AliasExistsException** error.

For more information about sign-in aliases, see [Customizing sign-in attributes](#).

Type: Boolean

Required: No

SecretHash

A keyed-hash message authentication code (HMAC) calculated using the secret key of a user pool client and username plus the client ID in the message. For more information about `SecretHash`, see [Computing secret hash values](#).

Type: String

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

Pattern: `[\w+=/+]`

Required: No

Session

The optional session ID from a `SignUp` API request. You can sign in a user directly from the sign-up process with the `USER_AUTH` authentication flow.

Type: String

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

Required: No

UserContextData

Contextual data about your user session like the device fingerprint, IP address, or location. Amazon Cognito threat protection evaluates the risk of an authentication event based on the context that your app generates and passes to Amazon Cognito when it makes API requests.

For more information, see [Collecting data for threat protection in applications](#).

Type: [UserContextDataType](#) object

Required: No

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

Response Syntax

```
{  
  "Session": "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.

Session

A session identifier that you can use to immediately sign in the confirmed user. You can automatically sign users in with the one-time password that they provided in a successful `ConfirmSignUp` request.

To do this, pass the `Session` parameter from this response in the `Session` parameter of an [InitiateAuth](#) or [AdminInitiateAuth](#) request.

Type: String

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

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AliasExistsException

This exception is thrown when a user tries to confirm the account with an email address or phone number that has already been supplied as an alias for a different user profile. This exception indicates that an account with this email address or phone already exists in a user pool that you've configured to use email address or phone number as a sign-in alias.

message

The message that Amazon Cognito sends to the user when the value of an alias attribute is already linked to another user profile.

HTTP Status Code: 400

CodeMismatchException

This exception is thrown if the provided code doesn't match what the server was expecting.

message

The message provided when the code mismatch exception is thrown.

HTTP Status Code: 400

ExpiredCodeException

This exception is thrown if a code has expired.

message

The message returned when the expired code exception is thrown.

HTTP Status Code: 400

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyFailedAttemptsException

This exception is thrown when the user has made too many failed attempts for a given action, such as sign-in.

message

The message returned when Amazon Cognito returns a TooManyFailedAttempts exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request confirms sign-up for the user "testuser" with the submitted confirmation code 123456. The response includes a session ID that your application can pass to [InitiateAuth](#) or [AdminInitiateAuth](#) for automatic email or SMS OTP sign-in with the already-submitted 123456 confirmation code.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ConfirmSignUp
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ClientId": "1example23456789",
  "ConfirmationCode": "123456",
  "Username": "testuser"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "Session": "AYABeC1-
y8qooiuysEv0uM4wAqQAHQABAAAdTZXJ2aWN1ABBDdb2duaXRvVXN1c1Bvb2xzAAEAB2F3cy1rbXMAS2Fybjphd3M6a21z0nV
}
```

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](#)

CreateGroup

Creates a new group in the specified user pool. For more information about user pool groups, see [Adding groups to a user pool](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "Description": "string",  
  "GroupName": "string",  
  "Precedence": number,  
  "RoleArn": "string",  
  "UserPoolId": "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.

Description

A description of the group that you're creating.

Type: String

Length Constraints: Maximum length of 2048.

Required: No

GroupName

A name for the group. This name must be unique in your user pool.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

Precedence

A non-negative integer value that specifies the precedence of this group relative to the other groups that a user can belong to in the user pool. Zero is the highest precedence value. Groups with lower Precedence values take precedence over groups with higher or null Precedence values. If a user belongs to two or more groups, it is the group with the lowest precedence value whose role ARN is given in the user's tokens for the `cognito:roles` and `cognito:preferred_role` claims.

Two groups can have the same Precedence value. If this happens, neither group takes precedence over the other. If two groups with the same Precedence have the same role ARN, that role is used in the `cognito:preferred_role` claim in tokens for users in each group. If the two groups have different role ARNs, the `cognito:preferred_role` claim isn't set in users' tokens.

The default Precedence value is null. The maximum Precedence value is $2^{31}-1$.

Type: Integer

Valid Range: Minimum value of 0.

Required: No

RoleArn

The Amazon Resource Name (ARN) for the IAM role that you want to associate with the group. A group role primarily declares a preferred role for the credentials that you get from an identity pool. Amazon Cognito ID tokens have a `cognito:preferred_role` claim that presents the

highest-precedence group that a user belongs to. Both ID and access tokens also contain a `cognito:groups` claim that list all the groups that a user is a member of.

Type: String

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

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

Required: No

UserPoolId

The ID of the user pool where you want to create a user group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "Group": {
    "CreationDate": number,
    "Description": "string",
    "GroupName": "string",
    "LastModifiedDate": number,
    "Precedence": number,
    "RoleArn": "string",
    "UserPoolId": "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.

Group

The response object for a created group.

Type: [GroupType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

GroupExistsException

This exception is thrown when Amazon Cognito encounters a group that already exists in the user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example creates the group `ExampleGroup` with precedence 1.

Sample Request

```
POST HTTP/1.1
```

```
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.CreateGroup
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "Description": "My Example Group",
  "GroupName": "ExampleGroup",
  "Precedence": 1,
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "Group": {
    "CreationDate": 1735240477.884,
    "Description": "My Example Group",
    "GroupName": "ExampleGroup",
    "LastModifiedDate": 1735240477.884,
    "Precedence": 1,
    "UserPoolId": "us-west-2_EXAMPLE"
  }
}
```

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](#)

CreateIdentityProvider

Adds a configuration and trust relationship between a third-party identity provider (IdP) and a user pool. Amazon Cognito accepts sign-in with third-party identity providers through managed login and OIDC relying-party libraries. For more information, see [Third-party IdP sign-in](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "AttributeMapping": {
    "string" : "string"
  },
  "IdpIdentifiers": [ "string" ],
  "ProviderDetails": {
    "string" : "string"
  },
  "ProviderName": "string",
  "ProviderType": "string",
  "UserPoolId": "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.

AttributeMapping

A mapping of IdP attributes to standard and custom user pool attributes. Specify a user pool attribute as the key of the key-value pair, and the IdP attribute claim name as the value.

Type: String to string map

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

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

IdpIdentifiers

An array of IdP identifiers, for example "IdpIdentifiers": ["MyIdP", "MyIdP2"]. Identifiers are friendly names that you can pass in the `idp_identifier` query parameter of requests to the [Authorize endpoint](#) to silently redirect to sign-in with the associated IdP. Identifiers in a domain format also enable the use of [email-address matching with SAML providers](#).

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 40.

Pattern: [`\w\s+=. @-`]+

Required: No

ProviderDetails

The scopes, URLs, and identifiers for your external identity provider. The following examples describe the provider detail keys for each IdP type. These values and their schema are subject to change. Social IdP `authorize_scopes` values must match the values listed here.

OpenID Connect (OIDC)

Amazon Cognito accepts the following elements when it can't discover endpoint URLs from `oidc_issuer`: `attributes_url`, `authorize_url`, `jwtks_uri`, `token_url`.

```
Create or update request: "ProviderDetails": { "attributes_request_method":  
"GET", "attributes_url": "https://auth.example.com/userInfo",  
"authorize_scopes": "openid profile email", "authorize_url": "https://
```

```
auth.example.com/authorize", "client_id": "1example23456789",  
"client_secret": "provider-app-client-secret", "jwks_uri": "https://  
auth.example.com/.well-known/jwks.json", "oidc_issuer": "https://  
auth.example.com", "token_url": "https://example.com/token" }
```

```
Describe response: "ProviderDetails": { "attributes_request_method":  
"GET", "attributes_url": "https://auth.example.com/userInfo",  
"attributes_url_add_attributes": "false", "authorize_scopes": "openid  
profile email", "authorize_url": "https://auth.example.com/authorize",  
"client_id": "1example23456789", "client_secret": "provider-app-  
client-secret", "jwks_uri": "https://auth.example.com/.well-known/  
jwks.json", "oidc_issuer": "https://auth.example.com", "token_url":  
"https://example.com/token" }
```

SAML

```
Create or update request with Metadata URL: "ProviderDetails": { "IDPInit":  
"true", "IDPSignout": "true", "EncryptedResponses" : "true",  
"MetadataURL": "https://auth.example.com/sso/saml/metadata",  
"RequestSigningAlgorithm": "rsa-sha256" }
```

```
Create or update request with Metadata file: "ProviderDetails": { "IDPInit":  
"true", "IDPSignout": "true", "EncryptedResponses" : "true",  
"MetadataFile": "[metadata XML]", "RequestSigningAlgorithm": "rsa-  
sha256" }
```

The value of `MetadataFile` must be the plaintext metadata document with all quote (") characters escaped by backslashes.

```
Describe response: "ProviderDetails": { "IDPInit": "true", "IDPSignout":  
"true", "EncryptedResponses" : "true", "ActiveEncryptionCertificate":  
"[certificate]", "MetadataURL": "https://auth.example.com/  
sso/saml/metadata", "RequestSigningAlgorithm": "rsa-sha256",  
"SLORedirectBindingURI": "https://auth.example.com/slo/saml",  
"SSORedirectBindingURI": "https://auth.example.com/sso/saml" }
```

LoginWithAmazon

```
Create or update request: "ProviderDetails": { "authorize_scopes":  
"profile postal_code", "client_id": "amzn1.application-oa2-
```

```
client.1example23456789", "client_secret": "provider-app-client-secret"
```

```
Describe response: "ProviderDetails": { "attributes_url": "https://api.amazon.com/user/profile", "attributes_url_add_attributes": "false", "authorize_scopes": "profile postal_code", "authorize_url": "https://www.amazon.com/ap/oa", "client_id": "amzn1.application-oa2-client.1example23456789", "client_secret": "provider-app-client-secret", "token_request_method": "POST", "token_url": "https://api.amazon.com/auth/o2/token" }
```

Google

```
Create or update request: "ProviderDetails": { "authorize_scopes": "email profile openid", "client_id": "1example23456789.apps.googleusercontent.com", "client_secret": "provider-app-client-secret" }
```

```
Describe response: "ProviderDetails": { "attributes_url": "https://people.googleapis.com/v1/people/me?personFields=", "attributes_url_add_attributes": "true", "authorize_scopes": "email profile openid", "authorize_url": "https://accounts.google.com/o/oauth2/v2/auth", "client_id": "1example23456789.apps.googleusercontent.com", "client_secret": "provider-app-client-secret", "oidc_issuer": "https://accounts.google.com", "token_request_method": "POST", "token_url": "https://www.googleapis.com/oauth2/v4/token" }
```

SignInWithApple

```
Create or update request: "ProviderDetails": { "authorize_scopes": "email name", "client_id": "com.example.cognito", "private_key": "1EXAMPLE", "key_id": "2EXAMPLE", "team_id": "3EXAMPLE" }
```

```
Describe response: "ProviderDetails": { "attributes_url_add_attributes": "false", "authorize_scopes": "email name", "authorize_url": "https://appleid.apple.com/auth/authorize", "client_id": "com.example.cognito", "key_id": "1EXAMPLE", "oidc_issuer": "https://appleid.apple.com", "team_id": "2EXAMPLE", "token_request_method": "POST", "token_url": "https://appleid.apple.com/auth/token" }
```


Facebook

Create or update request: "ProviderDetails": { "api_version": "v17.0",
"authorize_scopes": "public_profile, email", "client_id":
"1example23456789", "client_secret": "provider-app-client-secret" }

Describe response: "ProviderDetails": { "api_version": "v17.0",
"attributes_url": "https://graph.facebook.com/v17.0/me?fields=",
"attributes_url_add_attributes": "true", "authorize_scopes":
"public_profile, email", "authorize_url": "https://www.facebook.com/
v17.0/dialog/oauth", "client_id": "1example23456789", "client_secret":
"provider-app-client-secret", "token_request_method": "GET",
"token_url": "https://graph.facebook.com/v17.0/oauth/access_token" }

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: Yes

ProviderName

The name that you want to assign to the IdP. You can pass the identity provider name in the `identity_provider` query parameter of requests to the [Authorize endpoint](#) to silently redirect to sign-in with the associated IdP.

Type: String

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

Pattern: `[^_\\p{Z}][\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}][^_\\p{Z}]+`

Required: Yes

ProviderType

The type of IdP that you want to add. Amazon Cognito supports OIDC, SAML 2.0, Login With Amazon, Sign In With Apple, Google, and Facebook IdPs.

Type: String

Valid Values: SAML | Facebook | Google | LoginWithAmazon | SignInWithApple | OIDC

Required: Yes

UserPoolId

The Id of the user pool where you want to create an IdP.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "IdentityProvider": {
    "AttributeMapping": {
      "string" : "string"
    },
    "CreationDate": number,
    "IdpIdentifiers": [ "string" ],
    "LastModifiedDate": number,
    "ProviderDetails": {
      "string" : "string"
    },
    "ProviderName": "string",
    "ProviderType": "string",
    "UserPoolId": "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.

IdentityProvider

The details of the new user pool IdP.

Type: [IdentityProviderType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

DuplicateProviderException

This exception is thrown when the provider is already supported by the user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

This request adds a SAML IdP named MySAMLIdP to a user pool. The IdP is identified by a static `MetadataFile` in this request. Note the escape characters before the double-quotes in the metadata XML. You can also add a dynamic metadata source with `MetadataURL`. The SAML provider supports single logout (SLO) and provides the SLO endpoint in the metadata. Additionally, the SAML provider supports IdP-initiated SAML and encrypted responses.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-east-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.CreateIdentityProvider
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "AttributeMapping": {
    "email" : "idp_email",
    "email_verified" : "idp_email_verified"
  },
  "IdpIdentifiers": [ "platform" ],
  "ProviderDetails": {
    "MetadataFile": "<md:EntityDescriptor xmlns:md=
\"urn:oasis:names:tc:SAML:2.0:metadata\" entityID=\"http://www.example.com/saml
\"><md:IDPSSODescriptor WantAuthnRequestsSigned=\"false\" protocolSupportEnumeration=
\"urn:oasis:names:tc:SAML:2.0:protocol\"><md:KeyDescriptor use=
\"signing\"><ds:KeyInfo xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#
\"><ds:X509Data><ds:X509Certificate>CERTIFICATE_DATA</ds:X509Certificate></
ds:X509Data></ds:KeyInfo></md:KeyDescriptor><md:SingleLogoutService
  Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST\" Location=
\"https://example.com/slo/saml\"/><md:SingleLogoutService Binding=
\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\" Location=\"https://example.com/
slo/saml\"/><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</md:NameIDFormat><md:SingleSignOnService Binding=
\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST\" Location=\"https://example.com/sso/
saml\"/><md:SingleSignOnService Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect\" Location=\"https://example.com/sso/saml\"/></md:IDPSSODescriptor></
md:EntityDescriptor>\",
    "IDPSignout" : "true",
    "RequestSigningAlgorithm" : "rsa-sha256",
    "EncryptedResponses" : "true",
    "IDPInit" : "true"
  },
  "ProviderName": "MySAMLIdP",
  "ProviderType": "SAML",
  "UserPoolId": "us-east-1_EXAMPLE"
```

```
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "IdentityProvider": {
    "AttributeMapping": {
      "email": "idp_email",
      "email_verified": "idp_email_verified"
    },
    "CreationDate": 1701128513.249,
    "IdpIdentifiers": [
      "example.com"
    ],
    "LastModifiedDate": 1701128513.249,
    "ProviderDetails": {
      "MetadataFile": "<md:EntityDescriptor xmlns:md=
        \"urn:oasis:names:tc:SAML:2.0:metadata\" entityID=\"http://www.example.com/saml
        \"><md:IDPSSODescriptor WantAuthnRequestsSigned=\"false\" protocolSupportEnumeration=
        \"urn:oasis:names:tc:SAML:2.0:protocol\"><md:KeyDescriptor use=
        \"signing\"><ds:KeyInfo xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#
        \"><ds:X509Data><ds:X509Certificate>CERTIFICATE_DATA</ds:X509Certificate></
        ds:X509Data></ds:KeyInfo></md:KeyDescriptor><md:SingleLogoutService
        Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST\" Location=
        \"https://example.com/slo/saml\"/><md:SingleLogoutService Binding=
        \"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\" Location=\"https://example.com/
        slo/saml\"/><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
        md:NameIDFormat><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
        format:emailAddress</md:NameIDFormat><md:SingleSignOnService Binding=
        \"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST\" Location=\"https://example.com/sso/
        saml\"/><md:SingleSignOnService Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
        Redirect\" Location=\"https://example.com/sso/saml\"/></md:IDPSSODescriptor></
        md:EntityDescriptor>\",
      "IDPSignout" : "true",
      "RequestSigningAlgorithm" : "rsa-sha256",
```

```
        "EncryptedResponses" : "true",
        "IDPInit" : "true"
    },
    "ProviderName": "MySAMLIdP",
    "ProviderType": "SAML",
    "UserPoolId": "us-east-1_EXAMPLE"
}
}
```

Example

This request adds an OIDC IdP named MyOIDCIdP to a user pool. In this request, we have chosen not to discover the issuer endpoints with `oidc_issuer` but instead to enter them manually.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-east-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.CreateIdentityProvider
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "AttributeMapping": {
    "email" : "idp_email",
    "email_verified" : "idp_email_verified"
  },
  "IdpIdentifiers": [ "station" ],
  "ProviderDetails": {
    "attributes_request_method": "GET",
    "attributes_url": "https://example.com/userInfo",
    "attributes_url_add_attributes": "false",
    "authorize_scopes": "openid profile",
    "authorize_url": "https://example.com/authorize",
    "client_id": "idpexampleclient123",
    "client_secret": "idpexamplesecret456",
    "jwks_uri": "https://example.com/.well-known/jwks.json",
    "oidc_issuer": "https://example.com",
```

```
    "token_url": "https://example.com/token"
  },
  "ProviderName": "MyOIDCIdP",
  "ProviderType": "OIDC",
  "UserPoolId": "us-east-1_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "IdentityProvider": {
    "AttributeMapping": {
      "email": "idp_email",
      "email_verified": "idp_email_verified",
      "username": "sub"
    },
    "CreationDate": 1701129701.653,
    "IdpIdentifiers": [
      "station"
    ],
    "LastModifiedDate": 1701129701.653,
    "ProviderDetails": {
      "attributes_request_method": "GET",
      "attributes_url": "https://example.com/userInfo",
      "attributes_url_add_attributes": "false",
      "authorize_scopes": "openid profile",
      "authorize_url": "https://example.com/authorize",
      "client_id": "idpexampleclient123",
      "client_secret": "idpexamplesecret456",
      "jwks_uri": "https://example.com/.well-known/jwks.json",
      "oidc_issuer": "https://example.com",
      "token_url": "https://example.com/token"
    },
    "ProviderName": "MyOIDCIdP",
    "ProviderType": "OIDC",
```



```
"UserPoolId": "us-east-1_EXAMPLE"  
}  
}
```

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](#)

CreateManagedLoginBranding

Creates a new set of branding settings for a user pool style and associates it with an app client. This operation is the programmatic option for the creation of a new style in the branding editor.

Provides values for UI customization in a Settings JSON object and image files in an Assets array. To send the JSON object Document type parameter in Settings, you might need to update to the most recent version of your AWS SDK. To create a new style with default settings, set UseCognitoProvidedValues to true and don't provide values for any other options.

This operation has a 2-megabyte request-size limit and include the CSS settings and image assets for your app client. Your branding settings might exceed 2MB in size. Amazon Cognito doesn't require that you pass all parameters in one request and preserves existing style settings that you don't specify. If your request is larger than 2MB, separate it into multiple requests, each with a size smaller than the limit.

As a best practice, modify the output of [DescribeManagedLoginBrandingByClient](#) into the request parameters for this operation. To get all settings, set ReturnMergedResources to true. For more information, see [API and SDK operations for managed login branding](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "Assets": [
    {
      "Bytes": blob,
      "Category": "string",
```

```
    "ColorMode": "string",
    "Extension": "string",
    "ResourceId": "string"
  },
  "ClientId": "string",
  "Settings": JSON value,
  "UseCognitoProvidedValues": boolean,
  "UserPoolId": "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.

Assets

An array of image files that you want to apply to functions like backgrounds, logos, and icons. Each object must also indicate whether it is for dark mode, light mode, or browser-adaptive mode.

Type: Array of [AssetType](#) objects

Array Members: Minimum number of 0 items. Maximum number of 40 items.

Required: No

ClientId

The app client that you want to create the branding style for. Each style is linked to an app client until you delete it.

To change the style for an app client, delete the existing style with [DeleteManagedLoginBranding](#) and create a new one.

Type: String

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

Pattern: `[\w+]`

Required: Yes

Settings

A JSON file, encoded as a Document type, with the the settings that you want to apply to your style.

The following components are not currently implemented and reserved for future use:

- signUp
- instructions
- sessionTimerDisplay
- languageSelector (for localization, see [Managed login localization](#))

Type: JSON value

Required: No

UseCognitoProvidedValues

When true, applies the default branding style options. These default options are managed by Amazon Cognito. You can modify them later in the branding editor.

When you specify true for this option, you must also omit values for Settings and Assets in the request.

Type: Boolean

Required: No

UserPoolId

The ID of the user pool where you want to create a new branding style.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w- ]+_[0-9a-zA-Z ]+`

Required: Yes

Response Syntax

```
{
  "ManagedLoginBranding": {
```

```
"Assets": [
  {
    "Bytes": blob,
    "Category": "string",
    "ColorMode": "string",
    "Extension": "string",
    "ResourceId": "string"
  }
],
"CreationDate": number,
"LastModifiedDate": number,
"ManagedLoginBrandingId": "string",
"Settings": JSON value,
"UseCognitoProvidedValues": boolean,
"UserPoolId": "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.

ManagedLoginBranding

The details of the branding style that you created.

Type: [ManagedLoginBrandingType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

ManagedLoginBrandingExistsException

This exception is thrown when you attempt to apply a managed login branding style to an app client that already has an assigned style.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example creates a new managed login branding style for the app client with ID `1example23456789`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.ca-central-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.CreateManagedLoginBranding
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "Assets": [
    {
```

```

        "Bytes":
        "PHN2ZyB3aWR0aD0iMjAwMDAiIGhlaWdodD0iNDAwIiB2aWV3Qm94PSIwIDAgMjAwMDAgNDAwIiBmaWxsPSJub251IiB4b
+CjxyZWNoIHdpZHRoPSIyMDAwMCIgaGVpZ2h0PSI0MDAiIGZpbGw9InVybcGjcGFpbnQwX2xpbmVhcl8xNzI1OV8yMzY2Nz
+CjxsaW5lYXJHcmFkaWVudCBpZD0icGFpbnQwX2xpbmVhcl8xNzI1OV8yMzY2NzQiIHgxPSItODk0LjI0OSIgeTE9IjE5OS
+Cjwvc3ZnPgo=",
        "Category": "PAGE_FOOTER_BACKGROUND",
        "ColorMode": "DARK",
        "Extension": "SVG"
    }
],
"ClientId": "1example23456789",
"Settings": {
    "categories": {
        "auth": {
            "authMethodOrder": [
                [
                    {
                        "display": "BUTTON",
                        "type": "FEDERATED"
                    },
                    {
                        "display": "INPUT",
                        "type": "USERNAME_PASSWORD"
                    }
                ]
            ],
            "federation": {
                "interfaceStyle": "BUTTON_LIST",
                "order": [
                ]
            }
        },
        "form": {
            "displayGraphics": true,
            "instructions": {
                "enabled": false
            },
            "languageSelector": {
                "enabled": false
            },
            "location": {
                "horizontal": "CENTER",
                "vertical": "CENTER"
            }
        },

```



```
        "sessionTimerDisplay": "NONE"
    },
    "global": {
        "colorSchemeMode": "LIGHT",
        "pageFooter": {
            "enabled": false
        },
        "pageHeader": {
            "enabled": false
        },
        "spacingDensity": "REGULAR"
    },
    "signUp": {
        "acceptanceElements": [
            {
                "enforcement": "NONE",
                "textKey": "en"
            }
        ]
    }
},
"componentClasses": {
    "buttons": {
        "borderRadius": 8.0
    },
    "divider": {
        "darkMode": {
            "borderColor": "232b37ff"
        },
        "lightMode": {
            "borderColor": "ebebff"
        }
    },
    "dropDown": {
        "borderRadius": 8.0,
        "darkMode": {
            "defaults": {
                "itemBackgroundColor": "192534ff"
            },
            "hover": {
                "itemBackgroundColor": "081120ff",
                "itemBorderColor": "5f6b7aff",
                "itemTextColor": "e9ebedff"
            }
        }
    }
},
```

```
        "match": {
            "itemBackgroundColor": "d1d5dbff",
            "itemTextColor": "89bdeeff"
        },
    },
    "lightMode": {
        "defaults": {
            "itemBackgroundColor": "ffffffff"
        },
        "hover": {
            "itemBackgroundColor": "f4f4f4ff",
            "itemBorderColor": "7d8998ff",
            "itemTextColor": "000716ff"
        },
        "match": {
            "itemBackgroundColor": "414d5cff",
            "itemTextColor": "0972d3ff"
        }
    },
},
"focusState": {
    "darkMode": {
        "borderColor": "539fe5ff"
    },
    "lightMode": {
        "borderColor": "0972d3ff"
    }
},
"idpButtons": {
    "icons": {
        "enabled": true
    }
},
"input": {
    "borderRadius": 8.0,
    "darkMode": {
        "defaults": {
            "backgroundColor": "0f1b2aff",
            "borderColor": "5f6b7aff"
        },
        "placeholderColor": "8d99a8ff"
    },
    "lightMode": {
        "defaults": {
```

```
        "backgroundColor": "ffffffff",
        "borderColor": "7d8998ff"
    },
    "placeholderColor": "5f6b7aff"
}
},
"inputDescription": {
    "darkMode": {
        "textColor": "8d99a8ff"
    },
    "lightMode": {
        "textColor": "5f6b7aff"
    }
},
"inputLabel": {
    "darkMode": {
        "textColor": "d1d5dbff"
    },
    "lightMode": {
        "textColor": "000716ff"
    }
},
"link": {
    "darkMode": {
        "defaults": {
            "textColor": "539fe5ff"
        },
        "hover": {
            "textColor": "89bdeeff"
        }
    },
    "lightMode": {
        "defaults": {
            "textColor": "0972d3ff"
        },
        "hover": {
            "textColor": "033160ff"
        }
    }
},
"optionControls": {
    "darkMode": {
        "defaults": {
            "backgroundColor": "0f1b2aff",
```

```
        "borderColor": "7d8998ff"
      },
      "selected": {
        "backgroundColor": "539fe5ff",
        "foregroundColor": "000716ff"
      }
    },
    "lightMode": {
      "defaults": {
        "backgroundColor": "ffffffff",
        "borderColor": "7d8998ff"
      },
      "selected": {
        "backgroundColor": "0972d3ff",
        "foregroundColor": "ffffffff"
      }
    }
  },
  "statusIndicator": {
    "darkMode": {
      "error": {
        "backgroundColor": "1a0000ff",
        "borderColor": "eb6f6fff",
        "indicatorColor": "eb6f6fff"
      },
      "pending": {
        "indicatorColor": "AAAAAAAA"
      },
      "success": {
        "backgroundColor": "001a02ff",
        "borderColor": "29ad32ff",
        "indicatorColor": "29ad32ff"
      },
      "warning": {
        "backgroundColor": "1d1906ff",
        "borderColor": "e0ca57ff",
        "indicatorColor": "e0ca57ff"
      }
    },
    "lightMode": {
      "error": {
        "backgroundColor": "fff7f7ff",
        "borderColor": "d91515ff",
        "indicatorColor": "d91515ff"
      }
    }
  }
}
```

```
    },
    "pending": {
      "indicatorColor": "AAAAAAA"
    },
    "success": {
      "backgroundColor": "f2fcf3ff",
      "borderColor": "037f0cff",
      "indicatorColor": "037f0cff"
    },
    "warning": {
      "backgroundColor": "fffce9ff",
      "borderColor": "8d6605ff",
      "indicatorColor": "8d6605ff"
    }
  }
},
"components": {
  "alert": {
    "borderRadius": 12.0,
    "darkMode": {
      "error": {
        "backgroundColor": "1a0000ff",
        "borderColor": "eb6f6fff"
      }
    },
    "lightMode": {
      "error": {
        "backgroundColor": "fff7f7ff",
        "borderColor": "d91515ff"
      }
    }
  },
  "favicon": {
    "enabledTypes": [
      "ICO",
      "SVG"
    ]
  },
  "form": {
    "backgroundImage": {
      "enabled": false
    },
    "borderRadius": 8.0,
```

```
    "darkMode": {
      "backgroundColor": "0f1b2aff",
      "borderColor": "424650ff"
    },
    "lightMode": {
      "backgroundColor": "ffffffff",
      "borderColor": "c6c6cdff"
    },
    "logo": {
      "enabled": false,
      "formInclusion": "IN",
      "location": "CENTER",
      "position": "TOP"
    }
  },
  "idpButton": {
    "custom": {
    },
    "standard": {
      "darkMode": {
        "active": {
          "backgroundColor": "354150ff",
          "borderColor": "89bdeeff",
          "textColor": "89bdeeff"
        },
        "defaults": {
          "backgroundColor": "0f1b2aff",
          "borderColor": "c6c6cdff",
          "textColor": "c6c6cdff"
        },
        "hover": {
          "backgroundColor": "192534ff",
          "borderColor": "89bdeeff",
          "textColor": "89bdeeff"
        }
      },
      "lightMode": {
        "active": {
          "backgroundColor": "d3e7f9ff",
          "borderColor": "033160ff",
          "textColor": "033160ff"
        },
        "defaults": {
          "backgroundColor": "ffffffff",
```

```
        "borderColor": "424650ff",
        "textColor": "424650ff"
    },
    "hover": {
        "backgroundColor": "f2f8fdff",
        "borderColor": "033160ff",
        "textColor": "033160ff"
    }
}
},
"pageBackground": {
    "darkMode": {
        "color": "0f1b2aff"
    },
    "image": {
        "enabled": true
    },
    "lightMode": {
        "color": "ffffffff"
    }
},
"pageFooter": {
    "backgroundImage": {
        "enabled": false
    },
    "darkMode": {
        "background": {
            "color": "0f141aff"
        },
        "borderColor": "424650ff"
    },
    "lightMode": {
        "background": {
            "color": "fafafaff"
        },
        "borderColor": "d5dbdbff"
    },
    "logo": {
        "enabled": false,
        "location": "START"
    }
},
"pageHeader": {
```

```
    "backgroundImage": {
      "enabled": false
    },
    "darkMode": {
      "background": {
        "color": "0f141aff"
      },
      "borderColor": "424650ff"
    },
    "lightMode": {
      "background": {
        "color": "fafafaff"
      },
      "borderColor": "d5dbdbff"
    },
    "logo": {
      "enabled": false,
      "location": "START"
    }
  },
  "pageText": {
    "darkMode": {
      "bodyColor": "b6bec9ff",
      "descriptionColor": "b6bec9ff",
      "headingColor": "d1d5dbff"
    },
    "lightMode": {
      "bodyColor": "414d5cff",
      "descriptionColor": "414d5cff",
      "headingColor": "000716ff"
    }
  },
  "phoneNumberSelector": {
    "displayType": "TEXT"
  },
  "primaryButton": {
    "darkMode": {
      "active": {
        "backgroundColor": "539fe5ff",
        "textColor": "000716ff"
      },
      "defaults": {
        "backgroundColor": "539fe5ff",
        "textColor": "000716ff"
      }
    }
  }
}
```



```
    },
    "disabled": {
      "backgroundColor": "ffffffff",
      "borderColor": "ffffffff"
    },
    "hover": {
      "backgroundColor": "89bdeeff",
      "textColor": "000716ff"
    }
  },
  "lightMode": {
    "active": {
      "backgroundColor": "033160ff",
      "textColor": "ffffffff"
    },
    "defaults": {
      "backgroundColor": "0972d3ff",
      "textColor": "ffffffff"
    },
    "disabled": {
      "backgroundColor": "ffffffff",
      "borderColor": "ffffffff"
    },
    "hover": {
      "backgroundColor": "033160ff",
      "textColor": "ffffffff"
    }
  }
},
"secondaryButton": {
  "darkMode": {
    "active": {
      "backgroundColor": "354150ff",
      "borderColor": "89bdeeff",
      "textColor": "89bdeeff"
    },
    "defaults": {
      "backgroundColor": "0f1b2aff",
      "borderColor": "539fe5ff",
      "textColor": "539fe5ff"
    },
    "hover": {
      "backgroundColor": "192534ff",
      "borderColor": "89bdeeff",
```

```

        "textColor": "89bdeeff"
      },
    },
    "lightMode": {
      "active": {
        "backgroundColor": "d3e7f9ff",
        "borderColor": "033160ff",
        "textColor": "033160ff"
      },
      "defaults": {
        "backgroundColor": "ffffffff",
        "borderColor": "0972d3ff",
        "textColor": "0972d3ff"
      },
      "hover": {
        "backgroundColor": "f2f8fdff",
        "borderColor": "033160ff",
        "textColor": "033160ff"
      }
    }
  },
  "UseCognitoProvidedValues": false,
  "UserPoolId": "ca-central-1_EXAMPLE"
}

```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
```

```
{
  "ManagedLoginBranding": {
    "Assets": [
      {
        "Bytes":
"PHN2ZyB3aWR0aD0iMjAwMDAiIGhlawdodD0iNDAwIiB2aWV3Qm94PSIwIDAgMjAwMDAgNDAwIiBmaWxsPSJub251IiB4b
```

```

+CjxyZWN0IHdpZHRoPSIyMDAwMCIgaGVpZ2h0PSI0MDAiIGZpbGw9InVyY2NzI10V8yMzY2Nz
+CjxsaW5lYXJHcmFkaWVudCBpZD0icGFpbnQwX2xpbmVhc18xNzI10V8yMzY2NzQiIHgxPSIt
+Cjwvc3ZnPgo=",
    "Category": "PAGE_FOOTER_BACKGROUND",
    "ColorMode": "DARK",
    "Extension": "SVG"
  }
],
"CreationDate": 1732138490.642,
"LastModifiedDate": 1732140420.301,
"ManagedLoginBrandingId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
"Settings": {
  "categories": {
    "auth": {
      "authMethodOrder": [
        {
          "display": "BUTTON",
          "type": "FEDERATED"
        },
        {
          "display": "INPUT",
          "type": "USERNAME_PASSWORD"
        }
      ]
    },
    "federation": {
      "interfaceStyle": "BUTTON_LIST",
      "order": [
      ]
    }
  },
  "form": {
    "displayGraphics": true,
    "instructions": {
      "enabled": false
    },
    "languageSelector": {
      "enabled": false
    },
    "location": {
      "horizontal": "CENTER",
      "vertical": "CENTER"
    }
  },

```

```
        "sessionTimerDisplay": "NONE"
    },
    "global": {
        "colorSchemeMode": "LIGHT",
        "pageFooter": {
            "enabled": false
        },
        "pageHeader": {
            "enabled": false
        },
        "spacingDensity": "REGULAR"
    },
    "signUp": {
        "acceptanceElements": [
            {
                "enforcement": "NONE",
                "textKey": "en"
            }
        ]
    }
},
"componentClasses": {
    "buttons": {
        "borderRadius": 8.0
    },
    "divider": {
        "darkMode": {
            "borderColor": "232b37ff"
        },
        "lightMode": {
            "borderColor": "ebbf0ff"
        }
    },
    "dropDown": {
        "borderRadius": 8.0,
        "darkMode": {
            "defaults": {
                "itemBackgroundColor": "192534ff"
            },
            "hover": {
                "itemBackgroundColor": "081120ff",
                "itemBorderColor": "5f6b7aff",
                "itemTextColor": "e9ebedff"
            }
        }
    }
}
```

```
        "match": {
            "itemBackgroundColor": "d1d5dbff",
            "itemTextColor": "89bdeeff"
        },
    },
    "lightMode": {
        "defaults": {
            "itemBackgroundColor": "ffffffff"
        },
        "hover": {
            "itemBackgroundColor": "f4f4f4ff",
            "itemBorderColor": "7d8998ff",
            "itemTextColor": "000716ff"
        },
        "match": {
            "itemBackgroundColor": "414d5cff",
            "itemTextColor": "0972d3ff"
        }
    },
},
"focusState": {
    "darkMode": {
        "borderColor": "539fe5ff"
    },
    "lightMode": {
        "borderColor": "0972d3ff"
    }
},
"idpButtons": {
    "icons": {
        "enabled": true
    }
},
"input": {
    "borderRadius": 8.0,
    "darkMode": {
        "defaults": {
            "backgroundColor": "0f1b2aff",
            "borderColor": "5f6b7aff"
        },
        "placeholderColor": "8d99a8ff"
    },
    "lightMode": {
        "defaults": {
```

```
        "backgroundColor": "ffffffff",
        "borderColor": "7d8998ff"
    },
    "placeholderColor": "5f6b7aff"
}
},
"inputDescription": {
    "darkMode": {
        "textColor": "8d99a8ff"
    },
    "lightMode": {
        "textColor": "5f6b7aff"
    }
},
"inputLabel": {
    "darkMode": {
        "textColor": "d1d5dbff"
    },
    "lightMode": {
        "textColor": "000716ff"
    }
},
"link": {
    "darkMode": {
        "defaults": {
            "textColor": "539fe5ff"
        },
        "hover": {
            "textColor": "89bdeeff"
        }
    },
    "lightMode": {
        "defaults": {
            "textColor": "0972d3ff"
        },
        "hover": {
            "textColor": "033160ff"
        }
    }
},
"optionControls": {
    "darkMode": {
        "defaults": {
            "backgroundColor": "0f1b2aff",
```

```
        "borderColor": "7d8998ff"
      },
      "selected": {
        "backgroundColor": "539fe5ff",
        "foregroundColor": "000716ff"
      }
    },
    "lightMode": {
      "defaults": {
        "backgroundColor": "ffffffff",
        "borderColor": "7d8998ff"
      },
      "selected": {
        "backgroundColor": "0972d3ff",
        "foregroundColor": "ffffffff"
      }
    }
  },
  "statusIndicator": {
    "darkMode": {
      "error": {
        "backgroundColor": "1a0000ff",
        "borderColor": "eb6f6fff",
        "indicatorColor": "eb6f6fff"
      },
      "pending": {
        "indicatorColor": "AAAAAAAA"
      },
      "success": {
        "backgroundColor": "001a02ff",
        "borderColor": "29ad32ff",
        "indicatorColor": "29ad32ff"
      },
      "warning": {
        "backgroundColor": "1d1906ff",
        "borderColor": "e0ca57ff",
        "indicatorColor": "e0ca57ff"
      }
    },
    "lightMode": {
      "error": {
        "backgroundColor": "fff7f7ff",
        "borderColor": "d91515ff",
        "indicatorColor": "d91515ff"
      }
    }
  }
}
```

```
    },
    "pending": {
      "indicatorColor": "AAAAAAA"
    },
    "success": {
      "backgroundColor": "f2fcf3ff",
      "borderColor": "037f0cff",
      "indicatorColor": "037f0cff"
    },
    "warning": {
      "backgroundColor": "fffce9ff",
      "borderColor": "8d6605ff",
      "indicatorColor": "8d6605ff"
    }
  }
},
"components": {
  "alert": {
    "borderRadius": 12.0,
    "darkMode": {
      "error": {
        "backgroundColor": "1a0000ff",
        "borderColor": "eb6f6fff"
      }
    },
    "lightMode": {
      "error": {
        "backgroundColor": "fff7f7ff",
        "borderColor": "d91515ff"
      }
    }
  },
  "favicon": {
    "enabledTypes": [
      "ICO",
      "SVG"
    ]
  },
  "form": {
    "backgroundImage": {
      "enabled": false
    },
    "borderRadius": 8.0,
```



```
    "darkMode": {
      "backgroundColor": "0f1b2aff",
      "borderColor": "424650ff"
    },
    "lightMode": {
      "backgroundColor": "ffffffff",
      "borderColor": "c6c6cdff"
    },
    "logo": {
      "enabled": false,
      "formInclusion": "IN",
      "location": "CENTER",
      "position": "TOP"
    }
  },
  "idpButton": {
    "custom": {
    },
    "standard": {
      "darkMode": {
        "active": {
          "backgroundColor": "354150ff",
          "borderColor": "89bdeeff",
          "textColor": "89bdeeff"
        },
        "defaults": {
          "backgroundColor": "0f1b2aff",
          "borderColor": "c6c6cdff",
          "textColor": "c6c6cdff"
        },
        "hover": {
          "backgroundColor": "192534ff",
          "borderColor": "89bdeeff",
          "textColor": "89bdeeff"
        }
      },
      "lightMode": {
        "active": {
          "backgroundColor": "d3e7f9ff",
          "borderColor": "033160ff",
          "textColor": "033160ff"
        },
        "defaults": {
          "backgroundColor": "ffffffff",
```

```
        "borderColor": "424650ff",
        "textColor": "424650ff"
    },
    "hover": {
        "backgroundColor": "f2f8fdff",
        "borderColor": "033160ff",
        "textColor": "033160ff"
    }
}
},
"pageBackground": {
    "darkMode": {
        "color": "0f1b2aff"
    },
    "image": {
        "enabled": true
    },
    "lightMode": {
        "color": "ffffffff"
    }
},
"pageFooter": {
    "backgroundImage": {
        "enabled": false
    },
    "darkMode": {
        "background": {
            "color": "0f141aff"
        },
        "borderColor": "424650ff"
    },
    "lightMode": {
        "background": {
            "color": "fafafaff"
        },
        "borderColor": "d5dbdbff"
    },
    "logo": {
        "enabled": false,
        "location": "START"
    }
},
"pageHeader": {
```

```
    "backgroundImage": {
      "enabled": false
    },
    "darkMode": {
      "background": {
        "color": "0f141aff"
      },
      "borderColor": "424650ff"
    },
    "lightMode": {
      "background": {
        "color": "fafafaff"
      },
      "borderColor": "d5dbdbff"
    },
    "logo": {
      "enabled": false,
      "location": "START"
    }
  },
  "pageText": {
    "darkMode": {
      "bodyColor": "b6bec9ff",
      "descriptionColor": "b6bec9ff",
      "headingColor": "d1d5dbff"
    },
    "lightMode": {
      "bodyColor": "414d5cff",
      "descriptionColor": "414d5cff",
      "headingColor": "000716ff"
    }
  },
  "phoneNumberSelector": {
    "displayType": "TEXT"
  },
  "primaryButton": {
    "darkMode": {
      "active": {
        "backgroundColor": "539fe5ff",
        "textColor": "000716ff"
      },
      "defaults": {
        "backgroundColor": "539fe5ff",
        "textColor": "000716ff"
      }
    }
  }
}
```

```
    },
    "disabled": {
      "backgroundColor": "ffffffff",
      "borderColor": "ffffffff"
    },
    "hover": {
      "backgroundColor": "89bdeeff",
      "textColor": "000716ff"
    }
  },
  "lightMode": {
    "active": {
      "backgroundColor": "033160ff",
      "textColor": "ffffffff"
    },
    "defaults": {
      "backgroundColor": "0972d3ff",
      "textColor": "ffffffff"
    },
    "disabled": {
      "backgroundColor": "ffffffff",
      "borderColor": "ffffffff"
    },
    "hover": {
      "backgroundColor": "033160ff",
      "textColor": "ffffffff"
    }
  }
},
"secondaryButton": {
  "darkMode": {
    "active": {
      "backgroundColor": "354150ff",
      "borderColor": "89bdeeff",
      "textColor": "89bdeeff"
    },
    "defaults": {
      "backgroundColor": "0f1b2aff",
      "borderColor": "539fe5ff",
      "textColor": "539fe5ff"
    },
    "hover": {
      "backgroundColor": "192534ff",
      "borderColor": "89bdeeff",
```

```
        "textColor": "89bdeeff"
      },
    },
    "lightMode": {
      "active": {
        "backgroundColor": "d3e7f9ff",
        "borderColor": "033160ff",
        "textColor": "033160ff"
      },
      "defaults": {
        "backgroundColor": "ffffffff",
        "borderColor": "0972d3ff",
        "textColor": "0972d3ff"
      },
      "hover": {
        "backgroundColor": "f2f8fdff",
        "borderColor": "033160ff",
        "textColor": "033160ff"
      }
    }
  },
  "UseCognitoProvidedValues": false,
  "UserPoolId": "ca-central-1_EXAMPLE"
}
```

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](#)

CreateResourceServer

Creates a new OAuth2.0 resource server and defines custom scopes within it. Resource servers are associated with custom scopes and machine-to-machine (M2M) authorization. For more information, see [Access control with resource servers](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "Identifier": "string",
  "Name": "string",
  "Scopes": [
    {
      "ScopeDescription": "string",
      "ScopeName": "string"
    }
  ],
  "UserPoolId": "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.

Identifier

A unique resource server identifier for the resource server. The identifier can be an API friendly name like `solar-system-data`. You can also set an API URL like `https://solar-system-data-api.example.com` as your identifier.

Amazon Cognito represents scopes in the access token in the format `$resource-server-identifier/$scope`. Longer scope-identifier strings increase the size of your access tokens.

Type: String

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

Pattern: `[\x21\x23-\x5B\x5D-\x7E]+`

Required: Yes

Name

A friendly name for the resource server.

Type: String

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

Pattern: `[\w\s+=, .@- ]+`

Required: Yes

Scopes

A list of custom scopes. Each scope is a key-value map with the keys `ScopeName` and `ScopeDescription`. The name of a custom scope is a combination of `ScopeName` and the resource server Name in this request, for example `MyResourceServerName/MyScopeName`.

Type: Array of [ResourceServerScopeType](#) objects

Array Members: Maximum number of 100 items.

Required: No

UserPoolId

The ID of the user pool where you want to create a resource server.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "ResourceServer": {
    "Identifier": "string",
    "Name": "string",
    "Scopes": [
      {
        "ScopeDescription": "string",
        "ScopeName": "string"
      }
    ],
    "UserPoolId": "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.

ResourceServer

The details of the new resource server.

Type: [ResourceServerType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request creates a resource server for the API at `myapi.example.com` with the scopes `myapi.example.com/international.read` and `myapi.example.com/domestic.read`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.CreateResourceServer
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "Identifier": "myapi.example.com",
  "Name": "Example API with custom access control scopes",
  "Scopes": [
    {
      "ScopeDescription": "International customers",
      "ScopeName": "international.read"
    },
    {
      "ScopeDescription": "Domestic customers",
      "ScopeName": "domestic.read"
    }
  ]
}
```

```
    }  
  ],  
  "UserPoolId": "us-west-2_EXAMPLE"  
}
```

Sample Response

```
HTTP/1.1 200 OK  
Date: Tue, 13 Jun 2023 20:00:59 GMT  
Content-Type: application/x-amz-json-1.0  
Content-Length: <PayloadSizeBytes>  
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111  
Connection: keep-alive  
{  
  "ResourceServer": {  
    "Identifier": "myapi.example.com",  
    "Name": "Example API with custom access control scopes",  
    "Scopes": [  
      {  
        "ScopeDescription": "International customers",  
        "ScopeName": "international.read"  
      },  
      {  
        "ScopeDescription": "Domestic customers",  
        "ScopeName": "domestic.read"  
      }  
    ],  
    "UserPoolId": "us-west-2_EXAMPLE"  
  }  
}
```

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](#)

CreateTerms

Creates terms documents for the requested app client. When Terms and conditions and Privacy policy documents are configured, the app client displays links to them in the sign-up page of managed login for the app client.

You can provide URLs for terms documents in the languages that are supported by [managed login localization](#). Amazon Cognito directs users to the terms documents for their current language, with fallback to default if no document exists for the language.

Each request accepts one type of terms document and a map of language-to-link for that document type. You must provide both types of terms documents in at least one language before Amazon Cognito displays your terms documents. Supply each type in separate requests.

For more information, see [Terms documents](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "ClientId": "string",
  "Enforcement": "string",
  "Links": {
    "string" : "string"
  },
  "TermsName": "string",
  "TermsSource": "string",
  "UserPoolId": "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.

[ClientId](#)

The ID of the app client where you want to create terms documents. Must be an app client in the requested user pool.

Type: String

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

Pattern: `[\w+]`

Required: Yes

[Enforcement](#)

This parameter is reserved for future use and currently accepts only one value.

Type: String

Valid Values: NONE

Required: Yes

[Links](#)

A map of URLs to languages. For each localized language that will view the requested TermsName, assign a URL. A selection of `cognito:default` displays for all languages that don't have a language-specific URL.

For example, `"cognito:default": "https://terms.example.com",`
`"cognito:spanish": "https://terms.example.com/es".`

Type: String to string map

Map Entries: Maximum number of 12 items.

Key Pattern: `^cognito:(default|english|french|spanish|german|bahasa-indonesia|italian|japanese|korean|portuguese-brazil|chinese-(simplified|traditional))$`

Value Length Constraints: Minimum length of 1. Maximum length of 1024.

Value Pattern: `^[\p{L}\p{M}\p{S}\p{N}\p{P}]+$`

Required: No

TermsName

A friendly name for the document that you want to create in the current request. Must begin with `terms-of-use` or `privacy-policy` as identification of the document type. Provide URLs for both `terms-of-use` and `privacy-policy` in separate requests.

Type: String

Pattern: `^(terms-of-use|privacy-policy)$`

Required: Yes

TermsSource

This parameter is reserved for future use and currently accepts only one value.

Type: String

Valid Values: `LINK`

Required: Yes

UserPoolId

The ID of the user pool where you want to create terms documents.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{  
  "Terms": {  
    "ClientId": "string",
```



```
"CreationDate": number,
"Enforcement": "string",
"LastModifiedDate": number,
"Links": {
  "string" : "string"
},
"TermsId": "string",
"TermsName": "string",
"TermsSource": "string",
"UserPoolId": "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.

[Terms](#)

A summary of your terms documents. Includes a unique identifier for later changes to the terms documents.

Type: [TermsType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TermsExistsException

Terms document names must be unique to the app client. This exception is thrown when you attempt to create terms documents with a duplicate `TermsName`.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example operation creates a privacy policy terms document for app client `1example23456789` with URLs for default, French, and Portuguese (Brazil) languages.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.CreateTerms
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "ClientId": "1example23456789",
  "Enforcement": "NONE",
  "Links": {
    "cognito:default" : "https://example.com/privacy/",
```

```
"cognito:french" : "https://example.com/fr/privacy/",
"cognito:portuguese-brazil" : "https://example.com/pt/privacy/"
},
"TermsName": "privacy-policy",
"TermsSource": "LINK",
"UserPoolId": "us-east-1_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "Terms": {
    "ClientId": "1example23456789",
    "CreationDate": 1755793809.755,
    "Enforcement": "NONE",
    "LastModifiedDate": 1755793845.123,
    "Links": {
      "cognito:default": "https://example.com/privacy/",
      "cognito:french": "https://example.com/fr/privacy/",
      "cognito:portuguese-brazil": "https://example.com/pt/privacy/"
    },
    "TermsId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "TermsName": "privacy-policy",
    "TermsSource": "LINK",
    "UserPoolId": "us-east-1_EXAMPLE"
  }
}
```

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](#)

CreateUserImportJob

Creates a user import job. You can import users into user pools from a comma-separated values (CSV) file without adding Amazon Cognito MAU costs to your AWS bill.

To generate a template for your import, see [GetCSVHeader](#). To learn more about CSV import, see [Importing users from a CSV file](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "CloudWatchLogsRoleArn": "string",  
  "JobName": "string",  
  "UserPoolId": "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.

[CloudWatchLogsRoleArn](#)

You must specify an IAM role that has permission to log import-job results to Amazon CloudWatch Logs. This parameter is the ARN of that role.

Type: String

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

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

Required: Yes

JobName

A friendly name for the user import job.

Type: String

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

Pattern: `[\w\s+=, .@-]+`

Required: Yes

UserPoolId

The ID of the user pool that you want to import users into.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "UserImportJob": {
    "CloudWatchLogsRoleArn": "string",
    "CompletionDate": number,
    "CompletionMessage": "string",
    "CreationDate": number,
    "FailedUsers": number,
    "ImportedUsers": number,
    "JobId": "string",
    "JobName": "string",
```

```
"PreSignedUrl": "string",  
"SkippedUsers": number,  
"StartDate": number,  
"Status": "string",  
"UserPoolId": "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.

[UserImportJob](#)

The details of the user import job. Includes logging destination, status, and the Amazon S3 pre-signed URL for CSV upload.

Type: [UserImportJobType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PreconditionNotMetException

This exception is thrown when a precondition is not met.

message

The message returned when a precondition is not met.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request creates an import job in user pool `us-west-2_EXAMPLE`. The job will write log output to CloudWatch Logs with the IAM role `arn:aws:iam::123456789012:role/example-cloudwatch-logs-role`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.CreateUserImportJob
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/example-cloudwatch-logs-
role",
  "JobName": "Customer import",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
```

```
{
  "UserImportJob": {
    "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/example-cloudwatch-logs-
role",
    "CreationDate": 1735241621.022,
    "FailedUsers": 0,
    "ImportedUsers": 0,
    "JobId": "import-mAgUtd8PMm",
    "JobName": "Customer import",
    "PreSignedUrl": "https://aws-cognito-idp-user-import-pdx.s3.us-
west-2.amazonaws.com/123456789012/us-west-2_EXAMPLE/import-mAgUtd8PMm?X-Amz-Security-
Token=[token]&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20241226T193341Z&X-
Amz-SignedHeaders=host%3Bx-amz-server-side-encryption&X-Amz-Expires=899&X-Amz-
Credential=[credential]&X-Amz-Signature=[signature]",
    "SkippedUsers": 0,
    "Status": "Created",
    "UserPoolId": "us-west-2_EXAMPLE"
  }
}
```

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](#)

CreateUserPool

Creates a new Amazon Cognito user pool. This operation sets basic and advanced configuration options.

You can create a user pool in the Amazon Cognito console to your preferences and use the output of [DescribeUserPool](#) to generate requests from that baseline.

Important

If you don't provide a value for an attribute, Amazon Cognito sets it to its default value.

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)

- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "AccountRecoverySetting": {
    "RecoveryMechanisms": [
      {
        "Name": "string",
        "Priority": number
      }
    ]
  },
  "AdminCreateUserConfig": {
    "AllowAdminCreateUserOnly": boolean,
    "InviteMessageTemplate": {
      "EmailMessage": "string",
      "EmailSubject": "string",
      "SMSMessage": "string"
    },
    "UnusedAccountValidityDays": number
  },
  "AliasAttributes": [ "string" ],
  "AutoVerifiedAttributes": [ "string" ],
  "DeletionProtection": "string",
  "DeviceConfiguration": {
    "ChallengeRequiredOnNewDevice": boolean,
    "DeviceOnlyRememberedOnUserPrompt": boolean
  },
  "EmailConfiguration": {
    "ConfigurationSet": "string",
    "EmailSendingAccount": "string",
    "From": "string",
    "ReplyToEmailAddress": "string",
    "SourceArn": "string"
  },
  "EmailVerificationMessage": "string",
  "EmailVerificationSubject": "string",
  "LambdaConfig": {
    "CreateAuthChallenge": "string",
    "CustomEmailSender": {
```

```

    "LambdaArn": "string",
    "LambdaVersion": "string"
  },
  "CustomMessage": "string",
  "CustomSMSSender": {
    "LambdaArn": "string",
    "LambdaVersion": "string"
  },
  "DefineAuthChallenge": "string",
  "InboundFederation": {
    "LambdaArn": "string",
    "LambdaVersion": "string"
  },
  "KMSKeyID": "string",
  "PostAuthentication": "string",
  "PostConfirmation": "string",
  "PreAuthentication": "string",
  "PreSignUp": "string",
  "PreTokenGeneration": "string",
  "PreTokenGenerationConfig": {
    "LambdaArn": "string",
    "LambdaVersion": "string"
  },
  "UserMigration": "string",
  "VerifyAuthChallengeResponse": "string"
},
"MfaConfiguration": "string",
"Policies": {
  "PasswordPolicy": {
    "MinimumLength": number,
    "PasswordHistorySize": number,
    "RequireLowercase": boolean,
    "RequireNumbers": boolean,
    "RequireSymbols": boolean,
    "RequireUppercase": boolean,
    "TemporaryPasswordValidityDays": number
  },
  "SignInPolicy": {
    "AllowedFirstAuthFactors": [ "string" ]
  }
}
},
"PoolName": "string",
"Schema": [
  {

```

```

    "AttributeDataType": "string",
    "DeveloperOnlyAttribute": boolean,
    "Mutable": boolean,
    "Name": "string",
    "NumberAttributeConstraints": {
      "MaxValue": "string",
      "MinValue": "string"
    },
    "Required": boolean,
    "StringAttributeConstraints": {
      "MaxLength": "string",
      "MinLength": "string"
    }
  }
],
"SmsAuthenticationMessage": "string",
"SmsConfiguration": {
  "ExternalId": "string",
  "SnsCallerArn": "string",
  "SnsRegion": "string"
},
"SmsVerificationMessage": "string",
"UserAttributeUpdateSettings": {
  "AttributesRequireVerificationBeforeUpdate": [ "string" ]
},
"UsernameAttributes": [ "string" ],
"UsernameConfiguration": {
  "CaseSensitive": boolean
},
"UserPoolAddOns": {
  "AdvancedSecurityAdditionalFlows": {
    "CustomAuthMode": "string"
  },
  "AdvancedSecurityMode": "string"
},
"UserPoolTags": {
  "string" : "string"
},
"UserPoolTier": "string",
"VerificationMessageTemplate": {
  "DefaultEmailOption": "string",
  "EmailMessage": "string",
  "EmailMessageByLink": "string",
  "EmailSubject": "string",

```

```
    "EmailSubjectByLink": "string",  
    "SmsMessage": "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.

[AccountRecoverySetting](#)

The available verified method a user can use to recover their password when they call `ForgotPassword`. You can use this setting to define a preferred method when a user has more than one method available. With this setting, SMS doesn't qualify for a valid password recovery mechanism if the user also has SMS multi-factor authentication (MFA) activated. Email MFA is also disqualifying for account recovery with email. In the absence of this setting, Amazon Cognito uses the legacy behavior to determine the recovery method where SMS is preferred over email.

As a best practice, configure both `verified_email` and `verified_phone_number`, with one having a higher priority than the other.

Type: [AccountRecoverySettingType](#) object

Required: No

[AdminCreateUserConfig](#)

The configuration for administrative creation of users. Includes the template for the invitation message for new users, the duration of temporary passwords, and permitting self-service sign-up.

Type: [AdminCreateUserConfigType](#) object

Required: No

[AliasAttributes](#)

Attributes supported as an alias for this user pool. For more information about alias attributes, see [Customizing sign-in attributes](#).

Type: Array of strings

Valid Values: phone_number | email | preferred_username

Required: No

AutoVerifiedAttributes

The attributes that you want your user pool to automatically verify. For more information, see [Verifying contact information at sign-up](#).

Type: Array of strings

Valid Values: phone_number | email

Required: No

DeletionProtection

When active, DeletionProtection prevents accidental deletion of your user pool. Before you can delete a user pool that you have protected against deletion, you must deactivate this feature.

When you try to delete a protected user pool in a DeleteUserPool API request, Amazon Cognito returns an InvalidParameterException error. To delete a protected user pool, send a new DeleteUserPool request after you deactivate deletion protection in an UpdateUserPool API request.

Type: String

Valid Values: ACTIVE | INACTIVE

Required: No

DeviceConfiguration

The device-remembering configuration for a user pool. Device remembering or device tracking is a "Remember me on this device" option for user pools that perform authentication with the device key of a trusted device in the back end, instead of a user-provided MFA code. For more information about device authentication, see [Working with user devices in your user pool](#). A null value indicates that you have deactivated device remembering in your user pool.

Note

When you provide a value for any `DeviceConfiguration` field, you activate the Amazon Cognito device-remembering feature. For more information, see [Working with devices](#).

Type: [DeviceConfigurationType](#) object

Required: No

[EmailConfiguration](#)

The email configuration of your user pool. The email configuration type sets your preferred sending method, AWS Region, and sender for messages from your user pool.

Type: [EmailConfigurationType](#) object

Required: No

[EmailVerificationMessage](#)

This parameter is no longer used. See [VerificationMessageTemplateType](#).

This parameter is no longer used.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 20000.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s*]*\{####\}`
`[\p{L}\p{M}\p{S}\p{N}\p{P}\s*]*`

Required: No

[EmailVerificationSubject](#)

This parameter is no longer used. See [VerificationMessageTemplateType](#).

This parameter is no longer used.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 140.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s]+`

Required: No

LambdaConfig

A collection of user pool Lambda triggers. Amazon Cognito invokes triggers at several possible stages of authentication operations. Triggers can modify the outcome of the operations that invoked them.

Type: [LambdaConfigType](#) object

Required: No

MfaConfiguration

Sets multi-factor authentication (MFA) to be on, off, or optional. When ON, all users must set up MFA before they can sign in. When OPTIONAL, your application must make a client-side determination of whether a user wants to register an MFA device. For user pools with adaptive authentication with threat protection, choose OPTIONAL.

When MfaConfiguration is OPTIONAL, managed login doesn't automatically prompt users to set up MFA. Amazon Cognito generates MFA prompts in API responses and in managed login for users who have chosen and configured a preferred MFA factor.

Type: String

Valid Values: OFF | ON | OPTIONAL

Required: No

Policies

The password policy and sign-in policy in the user pool. The password policy sets options like password complexity requirements and password history. The sign-in policy sets the options available to applications in [choice-based authentication](#).

Type: [UserPoolPolicyType](#) object

Required: No

PoolName

A friendly name for your user pool.

Type: String

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

Pattern: `[\w\s+=, .@- ]+`

Required: Yes

Schema

An array of attributes for the new user pool. You can add custom attributes and modify the properties of default attributes. The specifications in this parameter set the required attributes in your user pool. For more information, see [Working with user attributes](#).

Type: Array of [SchemaAttributeType](#) objects

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

Required: No

SmsAuthenticationMessage

The contents of the SMS message that your user pool sends to users in SMS OTP and MFA authentication.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 140.

Pattern: `.*\{####\}.*`

Required: No

SmsConfiguration

The settings for your Amazon Cognito user pool to send SMS messages with Amazon Simple Notification Service. To send SMS messages with Amazon SNS in the AWS Region that you want, the Amazon Cognito user pool uses an AWS Identity and Access Management (IAM) role in your AWS account. For more information see [SMS message settings](#).

Type: [SmsConfigurationType](#) object

Required: No

SmsVerificationMessage

This parameter is no longer used. See [VerificationMessageTemplateType](#).

This parameter is no longer used.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 140.

Pattern: `.*\{####\}.*`

Required: No

UserAttributeUpdateSettings

The settings for updates to user attributes. These settings include the property `AttributesRequireVerificationBeforeUpdate`, a user-pool setting that tells Amazon Cognito how to handle changes to the value of your users' email address and phone number attributes. For more information, see [Verifying updates to email addresses and phone numbers](#).

Type: [UserAttributeUpdateSettingsType](#) object

Required: No

UsernameAttributes

Specifies whether a user can use an email address or phone number as a username when they sign up. For more information, see [Customizing sign-in attributes](#).

Type: Array of strings

Valid Values: `phone_number` | `email`

Required: No

UsernameConfiguration

Sets the case sensitivity option for sign-in usernames. When `CaseSensitive` is `false` (case insensitive), users can sign in with any combination of capital and lowercase letters. For example, `username`, `USERNAME`, or `UserName`, or for email, `email@example.com` or `EMail@eXampLE.Com`. For most use cases, set case sensitivity to `false` as a best practice. When usernames and email addresses are case insensitive, Amazon Cognito treats any variation in case as the same user, and prevents a case variation from being assigned to the same attribute for a different user.

When `CaseSensitive` is `true` (case sensitive), Amazon Cognito interprets `USERNAME` and `UserName` as distinct users.

This configuration is immutable after you set it.

Type: [UsernameConfigurationType](#) object

Required: No

UserPoolAddOns

Contains settings for activation of threat protection, including the operating mode and additional authentication types. To log user security information but take no action, set to AUDIT. To configure automatic security responses to potentially unwanted traffic to your user pool, set to ENFORCED.

For more information, see [Adding advanced security to a user pool](#). To activate this setting, your user pool must be on the [Plus tier](#).

Type: [UserPoolAddOnsType](#) object

Required: No

UserPoolTags

The tag keys and values to assign to the user pool. A tag is a label that you can use to categorize and manage user pools in different ways, such as by purpose, owner, environment, or other criteria.

Type: String to string map

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

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

Required: No

UserPoolTier

The user pool [feature plan](#), or tier. This parameter determines the eligibility of the user pool for features like managed login, access-token customization, and threat protection. Defaults to ESSENTIALS.

Type: String

Valid Values: LITE | ESSENTIALS | PLUS

Required: No

VerificationMessageTemplate

The template for the verification message that your user pool delivers to users who set an email address or phone number attribute.

Set the email message type that corresponds to your DefaultEmailOption selection. For CONFIRM_WITH_LINK, specify an EmailMessageByLink and leave EmailMessage blank. For CONFIRM_WITH_CODE, specify an EmailMessage and leave EmailMessageByLink blank. When you supply both parameters with either choice, Amazon Cognito returns an error.

Type: [VerificationMessageTemplateType](#) object

Required: No

Response Syntax

```
{
  "UserPool": {
    "AccountRecoverySetting": {
      "RecoveryMechanisms": [
        {
          "Name": "string",
          "Priority": number
        }
      ]
    },
    "AdminCreateUserConfig": {
      "AllowAdminCreateUserOnly": boolean,
      "InviteMessageTemplate": {
        "EmailMessage": "string",
        "EmailSubject": "string",
        "SMSMessage": "string"
      },
      "UnusedAccountValidityDays": number
    },
    "AliasAttributes": [ "string" ],
    "Arn": "string",
    "AutoVerifiedAttributes": [ "string" ],
    "CreationDate": number,
    "CustomDomain": "string",
    "DeletionProtection": "string",
    "DeviceConfiguration": {
      "ChallengeRequiredOnNewDevice": boolean,
      "DeviceOnlyRememberedOnUserPrompt": boolean
    },
    "Domain": "string",
    "EmailConfiguration": {
```

```
"ConfigurationSet": "string",
"EmailSendingAccount": "string",
"From": "string",
"ReplyToEmailAddress": "string",
"SourceArn": "string"
},
"EmailConfigurationFailure": "string",
"EmailVerificationMessage": "string",
"EmailVerificationSubject": "string",
"EstimatedNumberOfUsers": number,
"Id": "string",
"LambdaConfig": {
  "CreateAuthChallenge": "string",
  "CustomEmailSender": {
    "LambdaArn": "string",
    "LambdaVersion": "string"
  },
  "CustomMessage": "string",
  "CustomSMSSender": {
    "LambdaArn": "string",
    "LambdaVersion": "string"
  },
  "DefineAuthChallenge": "string",
  "InboundFederation": {
    "LambdaArn": "string",
    "LambdaVersion": "string"
  },
  "KMSKeyID": "string",
  "PostAuthentication": "string",
  "PostConfirmation": "string",
  "PreAuthentication": "string",
  "PreSignUp": "string",
  "PreTokenGeneration": "string",
  "PreTokenGenerationConfig": {
    "LambdaArn": "string",
    "LambdaVersion": "string"
  },
  "UserMigration": "string",
  "VerifyAuthChallengeResponse": "string"
},
"LastModifiedDate": number,
"MfaConfiguration": "string",
"Name": "string",
"Policies": {
```



```
"PasswordPolicy": {
  "MinimumLength": number,
  "PasswordHistorySize": number,
  "RequireLowercase": boolean,
  "RequireNumbers": boolean,
  "RequireSymbols": boolean,
  "RequireUppercase": boolean,
  "TemporaryPasswordValidityDays": number
},
"SignInPolicy": {
  "AllowedFirstAuthFactors": [ "string" ]
}
],
"SchemaAttributes": [
{
  "AttributeDataType": "string",
  "DeveloperOnlyAttribute": boolean,
  "Mutable": boolean,
  "Name": "string",
  "NumberAttributeConstraints": {
    "MaxValue": "string",
    "MinValue": "string"
  },
  "Required": boolean,
  "StringAttributeConstraints": {
    "MaxLength": "string",
    "MinLength": "string"
  }
}
],
"SmsAuthenticationMessage": "string",
"SmsConfiguration": {
  "ExternalId": "string",
  "SnsCallerArn": "string",
  "SnsRegion": "string"
},
"SmsConfigurationFailure": "string",
"SmsVerificationMessage": "string",
"Status": "string",
"UserAttributeUpdateSettings": {
  "AttributesRequireVerificationBeforeUpdate": [ "string" ]
},
"UsernameAttributes": [ "string" ],
"UsernameConfiguration": {
```

```

    "CaseSensitive": boolean
  },
  "UserPoolAddOns": {
    "AdvancedSecurityAdditionalFlows": {
      "CustomAuthMode": "string"
    },
    "AdvancedSecurityMode": "string"
  },
  "UserPoolTags": {
    "string" : "string"
  },
  "UserPoolTier": "string",
  "VerificationMessageTemplate": {
    "DefaultEmailOption": "string",
    "EmailMessage": "string",
    "EmailMessageByLink": "string",
    "EmailSubject": "string",
    "EmailSubjectByLink": "string",
    "SmsMessage": "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.

UserPool

The details of the created user pool.

Type: [UserPoolType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

FeatureUnavailableInTierException

This exception is thrown when a feature you attempted to configure isn't available in your current feature plan.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

TierChangeNotAllowedException

This exception is thrown when you've attempted to change your feature plan but the operation isn't permitted.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserPoolTaggingException

This exception is thrown when a user pool tag can't be set or updated.

HTTP Status Code: 400

Examples

Example

The following example creates a user pool with all configurable properties set to an example value. The resulting user pool allows sign-in with username or email address, has optional MFA, and has a Lambda function assigned to each possible trigger.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-east-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.CreateUserPool
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccountRecoverySetting": {
    "RecoveryMechanisms": [
      {
        "Name": "verified_email",
        "Priority": 1
      }
    ]
  },
  "AdminCreateUserConfig": {
    "AllowAdminCreateUserOnly": false,
    "InviteMessageTemplate": {
      "EmailMessage": "Your username is {username} and temporary password is
{####}.",
      "EmailSubject": "Your sign-in information",
```

```

    "SMSMessage": "Your username is {username} and temporary password is
{####}."
  },
  "AliasAttributes": [
    "email"
  ],
  "AutoVerifiedAttributes": [
    "email"
  ],
  "DeviceConfiguration": {
    "ChallengeRequiredOnNewDevice": true,
    "DeviceOnlyRememberedOnUserPrompt": true
  },
  "DeletionProtection": "ACTIVE",
  "EmailConfiguration": {
    "ConfigurationSet": "my-test-ses-configuration-set",
    "EmailSendingAccount": "DEVELOPER",
    "From": "support@example.com",
    "ReplyToEmailAddress": "support@example.com",
    "SourceArn": "arn:aws:ses:us-east-1:123456789012:identity/support@example.com"
  },
  "EmailVerificationMessage": "Your verification code is {####}.",
  "EmailVerificationSubject": "Verify your email address",
  "LambdaConfig": {
    "KMSKeyID": "arn:aws:kms:us-east-1:123456789012:key/
a6c4f8e2-0c45-47db-925f-87854bc9e357",
    "CustomEmailSender": {
      "LambdaArn": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
      "LambdaVersion": "V1_0"
    },
    "CustomSMSSender": {
      "LambdaArn": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
      "LambdaVersion": "V1_0"
    },
    "CustomMessage": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
    "DefineAuthChallenge": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
    "PostAuthentication": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
    "PostConfirmation": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
    "PreAuthentication": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",

```

```
    "PreSignUp": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
    "PreTokenGeneration": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
    "UserMigration": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
    "VerifyAuthChallengeResponse": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
    "InboundFederation": {
        "LambdaArn": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
        "LambdaVersion": "V1_0"
    }
},
"MfaConfiguration": "OPTIONAL",
"Policies": {
    "PasswordPolicy": {
        "MinimumLength": 6,
        "RequireLowercase": true,
        "RequireNumbers": true,
        "RequireSymbols": true,
        "RequireUppercase": true,
        "TemporaryPasswordValidityDays": 7
    },
    "SignInPolicy": {
        "AllowedFirstAuthFactors": [
            "PASSWORD",
            "EMAIL_OTP",
            "WEB_AUTHN"
        ]
    }
},
"PoolName": "my-test-user-pool",
"Schema": [
    {
        "AttributeDataType": "Number",
        "DeveloperOnlyAttribute": true,
        "Mutable": true,
        "Name": "mydev",
        "NumberAttributeConstraints": {
            "MaxValue": "99",
            "MinValue": "1"
        },
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "99",
            "MinLength": "1"
        }
    }
]
```

```

    }
  },
  "SmsAuthenticationMessage": "Your verification code is {####}.",
  "SmsConfiguration": {
    "ExternalId": "my-role-external-id",
    "SnsCallerArn": "arn:aws:iam::123456789012:role/service-role/test-cognito-SMS-Role"
  },
  "SmsVerificationMessage": "Your verification code is {####}.",
  "UserAttributeUpdateSettings": {
    "AttributesRequireVerificationBeforeUpdate": [
      "email"
    ]
  },
  "UsernameConfiguration": {
    "CaseSensitive": true
  },
  "UserPoolAddOns": {
    "AdvancedSecurityMode": "OFF"
  },
  "UserPoolTags": {
    "my-test-tag-key": "my-test-tag-key"
  },
  "UserPoolTier": "ESSENTIALS",
  "VerificationMessageTemplate": {
    "DefaultEmailOption": "CONFIRM_WITH_CODE",
    "EmailMessage": "Your confirmation code is {####}",
    "EmailMessageByLink": "Choose this link to {##verify your email##}",
    "EmailSubject": "Here is your confirmation code",
    "EmailSubjectByLink": "Here is your confirmation link",
    "SmsMessage": "Your confirmation code is {####}"
  }
}

```

Sample Response

```

HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

```



```

{
  "UserPool": {
    "AccountRecoverySetting": {
      "RecoveryMechanisms": [
        {
          "Name": "verified_email",
          "Priority": 1
        }
      ]
    },
    "AdminCreateUserConfig": {
      "AllowAdminCreateUserOnly": false,
      "InviteMessageTemplate": {
        "EmailMessage": "Your username is {username} and temporary password is
{#####}.",
        "EmailSubject": "Your sign-in information",
        "SMSMessage": "Your username is {username} and temporary password is
{#####}."
      },
      "UnusedAccountValidityDays": 7
    },
    "AliasAttributes": [
      "email"
    ],
    "Arn": "arn:aws:cognito-idp:us-east-1:123456789012:userpool/us-east-1_EXAMPLE",
    "AutoVerifiedAttributes": [
      "email"
    ],
    "CreationDate": 1689721665.239,
    "DeletionProtection": "ACTIVE",
    "DeviceConfiguration": {
      "ChallengeRequiredOnNewDevice": true,
      "DeviceOnlyRememberedOnUserPrompt": true
    },
    "EmailConfiguration": {
      "ConfigurationSet": "my-test-ses-configuration-set",
      "EmailSendingAccount": "DEVELOPER",
      "From": "support@example.com",
      "ReplyToEmailAddress": "support@example.com",
      "SourceArn": "arn:aws:ses:us-east-1:123456789012:identity/
support@example.com"
    },
    "EmailVerificationMessage": "Your verification code is {#####}.",
  }
}

```

```
    "EmailVerificationSubject": "Verify your email address",
    "EstimatedNumberOfUsers": 0,
    "Id": "us-east-1_EXAMPLE",
    "LambdaConfig": {
      "CustomEmailSender": {
        "LambdaArn": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
        "LambdaVersion": "V1_0"
      },
      "CustomMessage": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
      "CustomSMSSender": {
        "LambdaArn": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
        "LambdaVersion": "V1_0"
      },
      "DefineAuthChallenge": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
      "KMSKeyID": "arn:aws:kms:us-east-1:767671399759:key/4d43904c-8edf-4bb4-9fca-fb1a80e41cbe",
      "PostAuthentication": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
      "PostConfirmation": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
      "PreAuthentication": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
      "PreSignUp": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
      "PreTokenGeneration": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
      "UserMigration": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
      "VerifyAuthChallengeResponse": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
      "InboundFederation": {
        "LambdaArn": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
        "LambdaVersion": "V1_0"
      }
    },
    "LastModifiedDate": 1689721665.239,
    "MfaConfiguration": "OPTIONAL",
    "Name": "my-test-user-pool",
    "Policies": {
      "PasswordPolicy": {
```

```
        "MinimumLength": 6,
        "RequireLowercase": true,
        "RequireNumbers": true,
        "RequireSymbols": true,
        "RequireUppercase": true,
        "TemporaryPasswordValidityDays": 7
    }
},
"SchemaAttributes": [
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": false,
        "Name": "sub",
        "Required": true,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "1"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "name",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "given_name",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
```

```
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "family_name",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "middle_name",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "nickname",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "preferred_username",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
```

```
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "profile",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "picture",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "website",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "email",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "Boolean",
```

```
    "DeveloperOnlyAttribute": false,
    "Mutable": true,
    "Name": "email_verified",
    "Required": false
  },
  {
    "AttributeDataType": "String",
    "DeveloperOnlyAttribute": false,
    "Mutable": true,
    "Name": "gender",
    "Required": false,
    "StringAttributeConstraints": {
      "MaxLength": "2048",
      "MinLength": "0"
    }
  },
  {
    "AttributeDataType": "String",
    "DeveloperOnlyAttribute": false,
    "Mutable": true,
    "Name": "birthdate",
    "Required": false,
    "StringAttributeConstraints": {
      "MaxLength": "10",
      "MinLength": "10"
    }
  },
  {
    "AttributeDataType": "String",
    "DeveloperOnlyAttribute": false,
    "Mutable": true,
    "Name": "zoneinfo",
    "Required": false,
    "StringAttributeConstraints": {
      "MaxLength": "2048",
      "MinLength": "0"
    }
  },
  {
    "AttributeDataType": "String",
    "DeveloperOnlyAttribute": false,
    "Mutable": true,
    "Name": "locale",
    "Required": false,
```

```
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "phone_number",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "Boolean",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "phone_number_verify",
        "Required": false
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "address",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "Number",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "updated_at",
        "NumberAttributeConstraints": {
            "MinValue": "0"
        },
        "Required": false
    },
    },
```

```

    {
      "AttributeDataType": "Number",
      "DeveloperOnlyAttribute": true,
      "Mutable": true,
      "Name": "dev:custom:mydev",
      "NumberAttributeConstraints": {
        "MaxValue": "99",
        "MinValue": "1"
      },
      "Required": false
    }
  ],
  "SmsAuthenticationMessage": "Your verification code is {####}.",
  "SmsConfiguration": {
    "ExternalId": "my-role-external-id",
    "SnsCallerArn": "arn:aws:iam::123456789012:role/service-role/test-cognito-
SMS-Role",
    "SnsRegion": "us-east-1"
  },
  "SmsVerificationMessage": "Your verification code is {####}.",
  "UserAttributeUpdateSettings": {
    "AttributesRequireVerificationBeforeUpdate": [
      "email"
    ]
  },
  },
  "UserPoolAddOns": {
    "AdvancedSecurityMode": "OFF"
  },
  "UserPoolTags": {
    "my-test-tag-key": "my-test-tag-value"
  },
  "UserPoolTier": "ESSENTIALS",
  "UsernameConfiguration": {
    "CaseSensitive": true
  },
  "VerificationMessageTemplate": {
    "DefaultEmailOption": "CONFIRM_WITH_CODE",
    "EmailMessage": "Your confirmation code is {####}",
    "EmailMessageByLink": "Choose this link to {##verify your email##}",
    "EmailSubject": "Here is your confirmation code",
    "EmailSubjectByLink": "Here is your confirmation link",
    "SmsMessage": "Your confirmation code is {####}"
  }
}

```



```
}
```

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](#)

CreateUserPoolClient

Creates an app client in a user pool. This operation sets basic and advanced configuration options.

You can create an app client in the Amazon Cognito console to your preferences and use the output of [DescribeUserPoolClient](#) to generate requests from that baseline.

New app clients activate token revocation by default. For more information about revoking tokens, see [RevokeToken](#).

Unlike app clients created in the console, Amazon Cognito doesn't automatically assign a branding style to app clients that you configure with this API operation. Managed login and classic hosted UI pages aren't available for your client until after you apply a branding style.

Apply a branding style with the [CreateManagedLoginBranding](#) operation. For more information, see [Managed login branding](#).

Important

If you don't provide a value for an attribute, Amazon Cognito sets it to its default value.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "AccessTokenValidity": number,
```

```

"AllowedOAuthFlows": [ "string" ],
"AllowedOAuthFlowsUserPoolClient": boolean,
"AllowedOAuthScopes": [ "string" ],
"AnalyticsConfiguration": {
  "ApplicationArn": "string",
  "ApplicationId": "string",
  "ExternalId": "string",
  "RoleArn": "string",
  "UserDataShared": boolean
},
"AuthSessionValidity": number,
"CallbackURLs": [ "string" ],
"ClientName": "string",
"ClientSecret": "string",
"DefaultRedirectURI": "string",
"EnablePropagateAdditionalUserContextData": boolean,
"EnableTokenRevocation": boolean,
"ExplicitAuthFlows": [ "string" ],
"GenerateSecret": boolean,
"IdTokenValidity": number,
"LogoutURLs": [ "string" ],
"PreventUserExistenceErrors": "string",
"ReadAttributes": [ "string" ],
"RefreshTokenRotation": {
  "Feature": "string",
  "RetryGracePeriodSeconds": number
},
"RefreshTokenValidity": number,
"SupportedIdentityProviders": [ "string" ],
"TokenValidityUnits": {
  "AccessToken": "string",
  "IdToken": "string",
  "RefreshToken": "string"
},
"UserPoolId": "string",
"WriteAttributes": [ "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.

AccessTokenValidity

The access token time limit. After this limit expires, your user can't use their access token. To specify the time unit for `AccessTokenValidity` as seconds, minutes, hours, or days, set a `TokenValidityUnits` value in your API request.

For example, when you set `AccessTokenValidity` to 10 and `TokenValidityUnits` to hours, your user can authorize access with their access token for 10 hours.

The default time unit for `AccessTokenValidity` in an API request is hours. *Valid range* is displayed below in seconds.

If you don't specify otherwise in the configuration of your app client, your access tokens are valid for one hour.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 86400.

Required: No

AllowedOAuthFlows

The OAuth grant types that you want your app client to generate for clients in managed login authentication. To create an app client that generates client credentials grants, you must add `client_credentials` as the only allowed OAuth flow.

`code`

Use a code grant flow, which provides an authorization code as the response. This code can be exchanged for access tokens with the `/oauth2/token` endpoint.

`implicit`

Issue the access token, and the ID token when scopes like `openid` and `profile` are requested, directly to your user.

`client_credentials`

Issue the access token from the `/oauth2/token` endpoint directly to a non-person user, authorized by a combination of the client ID and client secret.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 3 items.

Valid Values: `code` | `implicit` | `client_credentials`

Required: No

AllowedOAuthFlowsUserPoolClient

Set to `true` to use OAuth 2.0 authorization server features in your app client.

This parameter must have a value of `true` before you can configure the following features in your app client.

- `CallbackURLs`: Callback URLs.
- `LogoutURLs`: Sign-out redirect URLs.
- `AllowedOAuthScopes`: OAuth 2.0 scopes.
- `AllowedOAuthFlows`: Support for authorization code, implicit, and client credentials OAuth 2.0 grants.

To use authorization server features, configure one of these features in the Amazon Cognito console or set `AllowedOAuthFlowsUserPoolClient` to `true` in a `CreateUserPoolClient` or `UpdateUserPoolClient` API request. If you don't set a value for `AllowedOAuthFlowsUserPoolClient` in a request with the AWS CLI or SDKs, it defaults to `false`. When `false`, only SDK-based API sign-in is permitted.

Type: Boolean

Required: No

AllowedOAuthScopes

The OAuth, OpenID Connect (OIDC), and custom scopes that you want to permit your app client to authorize access with. Scopes govern access control to user pool self-service API operations, user data from the `userInfo` endpoint, and third-party APIs. Scope values include `phone`, `email`, `openid`, and `profile`. The `aws.cognito.signin.user.admin` scope authorizes user self-service operations. Custom scopes with resource servers authorize access to external APIs.

Type: Array of strings

Array Members: Maximum number of 50 items.

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

Pattern: `[\x21\x23-\x5B\x5D-\x7E]+`

Required: No

AnalyticsConfiguration

The user pool analytics configuration for collecting metrics and sending them to your Amazon Pinpoint campaign.

In AWS Regions where Amazon Pinpoint isn't available, user pools might not have access to analytics or might be configurable with campaigns in the US East (N. Virginia) Region. For more information, see [Using Amazon Pinpoint analytics](#).

Type: [AnalyticsConfigurationType](#) object

Required: No

AuthSessionValidity

Amazon Cognito creates a session token for each API request in an authentication flow. `AuthSessionValidity` is the duration, in minutes, of that session token. Your user pool native user must respond to each authentication challenge before the session expires.

Type: Integer

Valid Range: Minimum value of 3. Maximum value of 15.

Required: No

CallbackURLs

A list of allowed redirect, or callback, URLs for managed login authentication. These URLs are the paths where you want to send your users' browsers after they complete authentication with managed login or a third-party IdP. Typically, callback URLs are the home of an application that uses OAuth or OIDC libraries to process authentication outcomes.

A redirect URI must meet the following requirements:

- Be an absolute URI.
- Be registered with the authorization server. Amazon Cognito doesn't accept authorization requests with `redirect_uri` values that aren't in the list of `CallbackURLs` that you provide in this parameter.

- Not include a fragment component.

See [OAuth 2.0 - Redirection Endpoint](#).

Amazon Cognito requires HTTPS over HTTP except for callback URLs to `http://localhost`, `http://127.0.0.1` and `http://[:1]`. These callback URLs are for testing purposes only. You can specify custom TCP ports for your callback URLs.

App callback URLs such as `myapp://example` are also supported.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: No

[ClientName](#)

A friendly name for the app client that you want to create.

Type: String

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

Pattern: `[\w\s+=, .@- ]+`

Required: Yes

[ClientSecret](#)

A custom client secret that you want to use for the app client. You cannot specify both `GenerateSecret` as `true` and provide a `ClientSecret` value.

Type: String

Length Constraints: Minimum length of 24. Maximum length of 64.

Pattern: `[\w+ ]+`

Required: No

DefaultRedirectURI

The default redirect URI. In app clients with one assigned IdP, replaces `redirect_uri` in authentication requests. Must be in the `CallbackURLs` list.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: No

EnablePropagateAdditionalUserData

When `true`, your application can include additional `UserContextData` in authentication requests. This data includes the IP address, and contributes to analysis by threat protection features. For more information about propagation of user context data, see [Adding session data to API requests](#). If you don't include this parameter, you can't send the source IP address to Amazon Cognito threat protection features. You can only activate `EnablePropagateAdditionalUserData` in an app client that has a client secret.

Type: Boolean

Required: No

EnableTokenRevocation

Activates or deactivates [token revocation](#) in the target app client.

Revoke tokens with [RevokeToken](#).

If you don't include this parameter, token revocation is automatically activated for the new user pool client.

Type: Boolean

Required: No

ExplicitAuthFlows

The [authentication flows](#) that you want your user pool client to support. For each app client in your user pool, you can sign in your users with any combination of one or more flows, including with a user name and Secure Remote Password (SRP), a user name and password, or a custom authentication process that you define with Lambda functions.

Note

If you don't specify a value for `ExplicitAuthFlows`, your app client supports `ALLOW_REFRESH_TOKEN_AUTH`, `ALLOW_USER_SRP_AUTH`, and `ALLOW_CUSTOM_AUTH`.

The values for authentication flow options include the following.

- `ALLOW_USER_AUTH`: Enable selection-based sign-in with `USER_AUTH`. This setting covers username-password, secure remote password (SRP), passwordless, and passkey authentication. This authentication flow can do username-password and SRP authentication without other `ExplicitAuthFlows` permitting them. For example users can complete an SRP challenge through `USER_AUTH` without the flow `USER_SRP_AUTH` being active for the app client. This flow doesn't include `CUSTOM_AUTH`.

To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

- `ALLOW_ADMIN_USER_PASSWORD_AUTH`: Enable admin based user password authentication flow `ADMIN_USER_PASSWORD_AUTH`. This setting replaces the `ADMIN_NO_SRP_AUTH` setting. With this authentication flow, your app passes a user name and password to Amazon Cognito in the request, instead of using the Secure Remote Password (SRP) protocol to securely transmit the password.
- `ALLOW_CUSTOM_AUTH`: Enable Lambda trigger based authentication.
- `ALLOW_USER_PASSWORD_AUTH`: Enable user password-based authentication. In this flow, Amazon Cognito receives the password in the request instead of using the SRP protocol to verify passwords.
- `ALLOW_USER_SRP_AUTH`: Enable SRP-based authentication.
- `ALLOW_REFRESH_TOKEN_AUTH`: Enable authflow to refresh tokens.

In some environments, you will see the values `ADMIN_NO_SRP_AUTH`, `CUSTOM_AUTH_FLOW_ONLY`, or `USER_PASSWORD_AUTH`. You can't assign these legacy `ExplicitAuthFlows` values to user pool clients at the same time as values that begin with `ALLOW_`, like `ALLOW_USER_SRP_AUTH`.

Type: Array of strings

Valid Values: `ADMIN_NO_SRP_AUTH` | `CUSTOM_AUTH_FLOW_ONLY` | `USER_PASSWORD_AUTH` | `ALLOW_ADMIN_USER_PASSWORD_AUTH` |

ALLOW_CUSTOM_AUTH | ALLOW_USER_PASSWORD_AUTH | ALLOW_USER_SRP_AUTH |
ALLOW_REFRESH_TOKEN_AUTH | ALLOW_USER_AUTH

Required: No

GenerateSecret

When `true`, generates a client secret for the app client. Client secrets are used with server-side and machine-to-machine applications. Client secrets are automatically generated; you can't specify a secret value. For more information, see [App client types](#).

Type: Boolean

Required: No

IdTokenValidity

The ID token time limit. After this limit expires, your user can't use their ID token. To specify the time unit for `IdTokenValidity` as seconds, minutes, hours, or days, set a `TokenValidityUnits` value in your API request.

For example, when you set `IdTokenValidity` as `10` and `TokenValidityUnits` as `hours`, your user can authenticate their session with their ID token for 10 hours.

The default time unit for `IdTokenValidity` in an API request is hours. *Valid range* is displayed below in seconds.

If you don't specify otherwise in the configuration of your app client, your ID tokens are valid for one hour.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 86400.

Required: No

LogoutURLs

A list of allowed logout URLs for managed login authentication. When you pass `logout_uri` and `client_id` parameters to `/logout`, Amazon Cognito signs out your user and redirects them to the logout URL. This parameter describes the URLs that you want to be the permitted targets of `logout_uri`. A typical use of these URLs is when a user selects "Sign out" and you redirect them to your public homepage. For more information, see [Logout endpoint](#).

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]`+

Required: No

PreventUserExistenceErrors

When ENABLED, suppresses messages that might indicate a valid user exists when someone attempts sign-in. This parameter sets your preference for the errors and responses that you want Amazon Cognito APIs to return during authentication, account confirmation, and password recovery when the user doesn't exist in the user pool. When set to ENABLED and the user doesn't exist, authentication returns an error indicating either the username or password was incorrect. Account confirmation and password recovery return a response indicating a code was sent to a simulated destination. When set to LEGACY, those APIs return a `UserNotFoundException` exception if the user doesn't exist in the user pool.

Defaults to LEGACY.

This setting affects the behavior of the following API operations.

- [AdminInitiateAuth](#)
- [AdminRespondToAuthChallenge](#)
- [InitiateAuth](#)
- [RespondToAuthChallenge](#)
- [ForgotPassword](#)
- [ConfirmForgotPassword](#)
- [ConfirmSignUp](#)
- [ResendConfirmationCode](#)

Type: String

Valid Values: LEGACY | ENABLED

Required: No

ReadAttributes

The list of user attributes that you want your app client to have read access to. After your user authenticates in your app, their access token authorizes them to read their own attribute value for any attribute in this list.

An example of this kind of activity is when your user selects a link to view their profile information. Your app makes a [GetUser](#) API request to retrieve and display your user's profile data.

When you don't specify the `ReadAttributes` for your app client, your app can read the values of `email_verified`, `phone_number_verified`, and the standard attributes of your user pool. When your user pool app client has read access to these default attributes, `ReadAttributes` doesn't return any information. Amazon Cognito only populates `ReadAttributes` in the API response if you have specified your own custom set of read attributes.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

RefreshTokenRotation

The configuration of your app client for refresh token rotation. When enabled, your app client issues new ID, access, and refresh tokens when users renew their sessions with refresh tokens. When disabled, token refresh issues only ID and access tokens.

Refresh token rotation must be completed with [GetTokensFromRefreshToken](#). With refresh token rotation disabled, you can complete token refresh with `GetTokensFromRefreshToken` and with `REFRESH_TOKEN_AUTH` in [InitiateAuth:AuthFlow](#) and [AdminInitiateAuth:AuthFlow](#).

Type: [RefreshTokenRotationType](#) object

Required: No

RefreshTokenValidity

The refresh token time limit. After this limit expires, your user can't use their refresh token. To specify the time unit for `RefreshTokenValidity` as seconds, minutes, hours, or days, set a `TokenValidityUnits` value in your API request.

For example, when you set `RefreshTokenValidity` as 10 and `TokenValidityUnits` as days, your user can refresh their session and retrieve new access and ID tokens for 10 days.

The default time unit for `RefreshTokenValidity` in an API request is days. You can't set `RefreshTokenValidity` to 0. If you do, Amazon Cognito overrides the value with the default value of 30 days. *Valid range* is displayed below in seconds.

If you don't specify otherwise in the configuration of your app client, your refresh tokens are valid for 30 days.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 315360000.

Required: No

SupportedIdentityProviders

A list of provider names for the identity providers (IdPs) that are supported on this client. The following are supported: COGNITO, Facebook, Google, SignInWithApple, and LoginWithAmazon. You can also specify the names that you configured for the SAML and OIDC IdPs in your user pool, for example MySAMLIdP or MyOIDCIdP.

This parameter sets the IdPs that [managed login](#) will display on the login page for your app client. The removal of COGNITO from this list doesn't prevent authentication operations for local users with the user pools API in an AWS SDK. The only way to prevent SDK-based authentication is to block access with a [AWS WAF rule](#).

Type: Array of strings

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\p{Z}]+`

Required: No

TokenValidityUnits

The units that validity times are represented in. The default unit for refresh tokens is days, and the default for ID and access tokens are hours.

Type: [TokenValidityUnitsType](#) object

Required: No

UserPoolId

The ID of the user pool where you want to create an app client.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

WriteAttributes

The list of user attributes that you want your app client to have write access to. After your user authenticates in your app, their access token authorizes them to set or modify their own attribute value for any attribute in this list.

An example of this kind of activity is when you present your user with a form to update their profile information and they change their last name. Your app then makes an [UpdateUserAttributes](#) API request and sets `family_name` to the new value.

When you don't specify the `WriteAttributes` for your app client, your app can write the values of the Standard attributes of your user pool. When your user pool has write access to these default attributes, `WriteAttributes` doesn't return any information. Amazon Cognito only populates `WriteAttributes` in the API response if you have specified your own custom set of write attributes.

If your app client allows users to sign in through an IdP, this array must include all attributes that you have mapped to IdP attributes. Amazon Cognito updates mapped attributes when users sign in to your application through an IdP. If your app client does not have write access to a mapped attribute, Amazon Cognito throws an error when it tries to update the attribute. For more information, see [Specifying IdP Attribute Mappings for Your user pool](#).

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

Response Syntax

```
{
  "UserPoolClient": {
    "AccessTokenValidity": number,
    "AllowedOAuthFlows": [ "string" ],
    "AllowedOAuthFlowsUserPoolClient": boolean,
    "AllowedOAuthScopes": [ "string" ],
    "AnalyticsConfiguration": {
      "ApplicationArn": "string",
      "ApplicationId": "string",
      "ExternalId": "string",
      "RoleArn": "string",
      "UserDataShared": boolean
    },
    "AuthSessionValidity": number,
    "CallbackURLs": [ "string" ],
    "ClientId": "string",
    "ClientName": "string",
    "ClientSecret": "string",
    "CreationDate": number,
    "DefaultRedirectURI": "string",
    "EnablePropagateAdditionalUserContextData": boolean,
    "EnableTokenRevocation": boolean,
    "ExplicitAuthFlows": [ "string" ],
    "IdTokenValidity": number,
    "LastModifiedDate": number,
    "LogoutURLs": [ "string" ],
    "PreventUserExistenceErrors": "string",
    "ReadAttributes": [ "string" ],
    "RefreshTokenRotation": {
      "Feature": "string",
      "RetryGracePeriodSeconds": number
    },
    "RefreshTokenValidity": number,
    "SupportedIdentityProviders": [ "string" ],
    "TokenValidityUnits": {
      "AccessToken": "string",
      "IdToken": "string",
      "RefreshToken": "string"
    },
    "UserPoolId": "string",
    "WriteAttributes": [ "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.

UserPoolClient

The details of the new app client.

Type: [UserPoolClientType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

FeatureUnavailableInTierException

This exception is thrown when a feature you attempted to configure isn't available in your current feature plan.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidOAuthFlowException

This exception is thrown when the specified OAuth flow is not valid.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

ScopeDoesNotExistException

This exception is thrown when the specified scope doesn't exist.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example creates an app client with all configurable properties set to an example value. The resulting user pool client connects to an analytics client, allows sign-in with username and password, and has two external identity providers associated with it.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-east-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.CreateUserPoolClient
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "AccessTokenValidity": 6,
  "AllowedOAuthFlows": [
    "code"
  ],
  "AllowedOAuthFlowsUserPoolClient": true,
  "AllowedOAuthScopes": [
    "aws.cognito.signin.user.admin",
    "openid"
  ],
  "AnalyticsConfiguration": {
    "ApplicationId": "d70b2ba36a8c4dc5a04a0451a31a1e12",
    "ExternalId": "my-external-id",
    "RoleArn": "arn:aws:iam::123456789012:role/test-cognitouserpool-role",
    "UserDataShared": true
  }
}
```

```
{,
  "CallbackURLs": [
    "https://example.com",
    "http://localhost",
    "myapp://example"
  ],
  "ClientName": "my-test-app-client",
  "DefaultRedirectURI": "https://example.com",
  "ExplicitAuthFlows": [
    "ALLOW_USER_AUTH",
    "ALLOW_ADMIN_USER_PASSWORD_AUTH",
    "ALLOW_USER_PASSWORD_AUTH",
    "ALLOW_REFRESH_TOKEN_AUTH"
  ],
  "GenerateSecret": true,
  "IdTokenValidity": 6,
  "LogoutURLs": [
    "https://example.com/logout"
  ],
  "PreventUserExistenceErrors": "ENABLED",
  "ReadAttributes": [
    "email",
    "address",
    "preferred_username"
  ],
  "RefreshTokenValidity": 6,
  "SupportedIdentityProviders": [
    "SignInWithApple",
    "MySSO"
  ],
  "TokenValidityUnits": {
    "AccessToken": "hours",
    "IdToken": "minutes",
    "RefreshToken": "days"
  },
  "UserPoolId": "us-east-1_EXAMPLE",
  "WriteAttributes": [
    "family_name",
    "email"
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "UserPoolClient": {
    "AccessTokenValidity": 6,
    "AllowedOAuthFlows": [
      "code"
    ],
    "AllowedOAuthFlowsUserPoolClient": true,
    "AllowedOAuthScopes": [
      "aws.cognito.signin.user.admin",
      "openid"
    ],
    "AnalyticsConfiguration": {
      "ApplicationId": "d70b2ba36a8c4dc5a04a0451a31a1e12",
      "ExternalId": "my-external-id",
      "RoleArn": "arn:aws:iam::123456789012:role/test-cognitouserpool-role",
      "UserDataShared": true
    },
    "AuthSessionValidity": 3,
    "CallbackURLs": [
      "https://example.com",
      "http://localhost",
      "myapp://example"
    ],
    "ClientId": "1example23456789",
    "ClientName": "my-test-app-client",
    "ClientSecret": "13ka4h7u28d9oo44tqpq9djqsfvhvu8rk4d2ighvpu0k8fj1c2r9",
    "CreationDate": 1689885426.107,
    "DefaultRedirectURI": "https://example.com",
    "EnablePropagateAdditionalUserContextData": false,
    "EnableTokenRevocation": true,
    "ExplicitAuthFlows": [
      "ALLOW_USER_AUTH",
      "ALLOW_USER_PASSWORD_AUTH",
      "ALLOW_ADMIN_USER_PASSWORD_AUTH",
      "ALLOW_REFRESH_TOKEN_AUTH"
    ]
  }
}
```

```
    ],
    "IdTokenValidity": 6,
    "LastModifiedDate": 1689885426.107,
    "LogoutURLs": [
      "https://example.com/logout"
    ],
    "PreventUserExistenceErrors": "ENABLED",
    "ReadAttributes": [
      "address",
      "preferred_username",
      "email"
    ],
    "RefreshTokenValidity": 6,
    "SupportedIdentityProviders": [
      "SignInWithApple",
      "MySSO"
    ],
    "TokenValidityUnits": {
      "AccessToken": "hours",
      "IdToken": "minutes",
      "RefreshToken": "days"
    },
    "UserPoolId": "us-east-1_EXAMPLE",
    "WriteAttributes": [
      "family_name",
      "email"
    ]
  ]
}
```

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](#)

CreateUserPoolDomain

A user pool domain hosts managed login, an authorization server and web server for authentication in your application. This operation creates a new user pool prefix domain or custom domain and sets the managed login branding version. Set the branding version to 1 for hosted UI (classic) or 2 for managed login. When you choose a custom domain, you must provide an SSL certificate in the US East (N. Virginia) AWS Region in your request.

Your prefix domain might take up to one minute to take effect. Your custom domain is online within five minutes, but it can take up to one hour to distribute your SSL certificate.

For more information about adding a custom domain to your user pool, see [Configuring a user pool domain](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "CustomDomainConfig": {
    "CertificateArn": "string"
  },
  "Domain": "string",
  "ManagedLoginVersion": number,
  "UserPoolId": "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.

CustomDomainConfig

The configuration for a custom domain. Configures your domain with an AWS Certificate Manager certificate in the us-east-1 Region.

Provide this parameter only if you want to use a [custom domain](#) for your user pool. Otherwise, you can omit this parameter and use a [prefix domain](#) instead.

When you create a custom domain, the passkey RP ID defaults to the custom domain. If you had a prefix domain active, this will cause passkey integration for your prefix domain to stop working due to a mismatch in RP ID. To keep the prefix domain passkey integration working, you can explicitly set RP ID to the prefix domain.

Update the RP ID in a [SetUserPoolMfaConfig](#) request.

Type: [CustomDomainConfigType](#) object

Required: No

Domain

The domain string. For custom domains, this is the fully-qualified domain name, such as `auth.example.com`. For prefix domains, this is the prefix alone, such as `myprefix`. A prefix value of `myprefix` for a user pool in the us-east-1 Region results in a domain of `myprefix.auth.us-east-1.amazoncognito.com`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 63.

Pattern: `^[a-z0-9](?:[a-z0-9\-\]{0,61}[a-z0-9])?$`

Required: Yes

ManagedLoginVersion

The version of managed login branding that you want to apply to your domain. A value of 1 indicates hosted UI (classic) and a version of 2 indicates managed login.

Managed login requires that your user pool be configured for any [feature plan](#) other than Lite.

Type: Integer

Required: No

UserPoolId

The ID of the user pool where you want to add a domain.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "CloudFrontDomain": "string",
  "ManagedLoginVersion": 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.

CloudFrontDomain

The fully-qualified domain name (FQDN) of the Amazon CloudFront distribution that hosts your managed login or classic hosted UI pages. Your domain-name authority must have an alias record that points requests for your custom domain to this FQDN. Amazon Cognito returns this value if you set a custom domain with `CustomDomainConfig`. If you set an Amazon Cognito prefix domain, this parameter returns null.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 63.

Pattern: `^[a-z0-9](?:[a-z0-9\-\_]{0,61}[a-z0-9])?$`

ManagedLoginVersion

The version of managed login branding applied your domain. A value of 1 indicates hosted UI (classic) and a version of 2 indicates managed login.

Type: Integer

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

FeatureUnavailableInTierException

This exception is thrown when a feature you attempted to configure isn't available in your current feature plan.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

Examples

Example

The following example creates a user pool custom domain. Amazon Cognito creates resources for the resulting domain `auth.example.com` at the CloudFront distribution `example.cloudfront.net`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.ca-central-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.CreateUserPoolDomain
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "CustomDomainConfig": {
    "CertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Domain": "auth.example.com",
  "ManagedLoginVersion": 2,
  "UserPoolId": "ca-central-1_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "CloudFrontDomain": "example.cloudfront.net",
  "ManagedLoginVersion": 2
}
```

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](#)

DeleteGroup

Deletes a group from the specified user pool. When you delete a group, that group no longer contributes to users' `cognito:preferred_group` or `cognito:groups` claims, and no longer influence access-control decision that are based on group membership. For more information about user pool groups, see [Adding groups to a user pool](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "GroupName": "string",  
  "UserPoolId": "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.

GroupName

The name of the group that you want to delete.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to delete the group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request deletes the group `ExampleGroup` in the user pool `us-west-2_EXAMPLE`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
```



```
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DeleteGroup
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "GroupName": "ExampleGroup",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

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](#)

DeleteIdentityProvider

Deletes a user pool identity provider (IdP). After you delete an IdP, users can no longer sign in to your user pool through that IdP. For more information about user pool IdPs, see [Third-party IdP sign-in](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "ProviderName": "string",  
  "UserPoolId": "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.

[ProviderName](#)

The name of the IdP that you want to delete.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\p{Z}]`+

Required: Yes

UserPoolId

The ID of the user pool where you want to delete the identity provider.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnsupportedIdentityProviderException

This exception is thrown when the specified identifier isn't supported.

HTTP Status Code: 400

Examples

Example

The following example request deletes the IdP MyIdP in user pool us-west-2_EXAMPLE.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DeleteIdentityProvider
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ProviderName": "MyIdP",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

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](#)

DeleteManagedLoginBranding

Deletes a managed login branding style. When you delete a style, you delete the branding association for an app client. When an app client doesn't have a style assigned, your managed login pages for that app client are nonfunctional until you create a new style or switch the domain branding version.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "ManagedLoginBrandingId": "string",  
  "UserPoolId": "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.

[ManagedLoginBrandingId](#)

The ID of the managed login branding style that you want to delete.

Type: String

Pattern: `^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[4][0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}$`

Required: Yes

UserPoolId

The ID of the user pool that contains the managed login branding style that you want to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request deletes the managed login style with ID `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111` from user pool `us-west-2_EXAMPLE`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DeleteManagedLoginBranding
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ManagedLoginBrandingId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

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](#)

DeleteResourceServer

Deletes a resource server. After you delete a resource server, users can no longer generate access tokens with scopes that are associate with that resource server.

Resource servers are associated with custom scopes and machine-to-machine (M2M) authorization. For more information, see [Access control with resource servers](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "Identifier": "string",
  "UserPoolId": "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.

Identifier

The identifier of the resource server that you want to delete.

Type: String

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

Pattern: `[\x21\x23-\x5B\x5D-\x7E]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to delete the resource server.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request deletes the resource server MyAPI from user pool us-west-2_EXAMPLE.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
```

```
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DeleteResourceServer
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "Identifier": "MyAPI",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

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](#)

DeleteTerms

Deletes the terms documents with the requested ID from your app client.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "TermsId": "string",  
  "UserPoolId": "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.

[TermsId](#)

The ID of the terms documents that you want to delete.

Type: String

Pattern: `^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[4][0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}$`

Required: Yes

UserPoolId

The ID of the user pool that contains the terms documents that you want to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example operation deletes a terms document with the specified TermsId.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DeleteTerms
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "TermsId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "UserPoolId": "us-east-1_EXAMPLE"
}
```

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](#)

DeleteUser

Deletes the profile of the currently signed-in user. A deleted user profile can no longer be used to sign in and can't be restored.

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{  
  "AccessToken": "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.

[AccessToken](#)

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: `[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](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request deletes the user with the access token eyJra456defEXAMPLE.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DeleteUser
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE"
}
```

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](#)

DeleteUserAttributes

Deletes attributes from the currently signed-in user. For example, your application can submit a request to this operation when a user wants to remove their birthdate attribute value.

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{
  "AccessToken": "string",
  "UserAttributeNames": [ "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.

AccessToken

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: Yes

UserAttributeNames

An array of strings representing the user attribute names you want to delete.

For custom attributes, you must prepend the `custom:` prefix to the attribute name, for example `custom:department`.

Type: Array of strings

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\t\n\r ]+`

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](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request deletes the attributes `nickname` and `middle_name` from the user with the access token `eyJra456defEXAMPLE`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DeleteUserAttributes
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
```

```
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE",
  "UserAttributeNames": [
    "nickname",
    "middle_name"
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

DeleteUserPool

Deletes a user pool. After you delete a user pool, users can no longer sign in to any associated applications.

When you delete a user pool, it's no longer visible or operational in your AWS account. Amazon Cognito retains deleted user pools in an inactive state for 14 days, then begins a cleanup process that fully removes them from AWS systems. In case of accidental deletion, contact Support within 14 days for restoration assistance.

Amazon Cognito begins full deletion of all resources from deleted user pools after 14 days. In the case of large user pools, the cleanup process might take significant additional time before all user data is permanently deleted.

Request Syntax

```
{  
  "UserPoolId": "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.

UserPoolId

The ID of the user pool that you want to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w- ]+_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserImportInProgressException

This exception is thrown when you're trying to modify a user pool while a user import job is in progress for that pool.

message

The message returned when the user pool has an import job running.

HTTP Status Code: 400

Examples

Example

The following example request doesn't succeed in deletion of the user pool `us-west-2_EXAMPLE` because deletion protection is active.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DeleteUserPool
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "__type": "InvalidParameterException",
  "message": "User pool cannot be deleted. It has a domain configured that should be
  deleted first."
}
```

Example

The following example request deletes the user pool `us-west-2_EXAMPLE` after deletion protection is inactive.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DeleteUserPool
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

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](#)

DeleteUserPoolClient

Deletes a user pool app client. After you delete an app client, users can no longer sign in to the associated application.

Request Syntax

```
{  
  "ClientId": "string",  
  "UserPoolId": "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.

ClientId

The ID of the user pool app client that you want to delete.

Type: String

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

Pattern: `[\w+]`

Required: Yes

UserPoolId

The ID of the user pool where you want to delete the client.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request deletes the user pool client with ID 1example23456789 from user pool us-west-2_EXAMPLE.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DeleteUserPoolClient
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
```

```
Content-Length: <PayloadSizeBytes>
{
  "ClientId": "1example23456789",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

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](#)

DeleteUserPoolClientSecret

Deletes a specific client secret from a user pool app client. You cannot delete the last remaining secret for an app client.

Request Syntax

```
{  
  "ClientId": "string",  
  "ClientSecretId": "string",  
  "UserPoolId": "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.

ClientId

The ID of the app client from which you want to delete the secret.

Type: String

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

Pattern: `[\w+]`

Required: Yes

ClientSecretId

The unique identifier of the client secret you want to delete.

Type: String

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

Required: Yes

UserPoolId

The ID of the user pool that contains the app client.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w- ]+_[0-9a-zA-Z]+`

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](#).

InternalServerErrorException

This exception is thrown when Amazon Cognito encounters an internal server error.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

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](#)

DeleteUserPoolDomain

Given a user pool ID and domain identifier, deletes a user pool domain. After you delete a user pool domain, your managed login pages and authorization server are no longer available.

Request Syntax

```
{  
  "Domain": "string",  
  "UserPoolId": "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.

Domain

The domain that you want to delete. For custom domains, this is the fully-qualified domain name like `auth.example.com`. For Amazon Cognito prefix domains, this is the prefix alone, like `myprefix`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 63.

Pattern: `^[a-z0-9](?:[a-z0-9\-\]{0,61}[a-z0-9])?$`

Required: Yes

UserPoolId

The ID of the user pool where you want to delete the domain.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

Examples

Example

The following example request deletes the Amazon Cognito prefix domain mytestdomain from the user pool us-west-2_EXAMPLE.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DeleteUserPoolDomain
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "Domain": "mytestdomain",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
```

```
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

DeleteWebAuthnCredential

Deletes a registered passkey, or WebAuthn, authenticator for the currently signed-in user.

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{  
  "AccessToken": "string",  
  "CredentialId": "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.

AccessToken

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: Yes

CredentialId

The unique identifier of the passkey that you want to delete.

Look up registered devices with [ListWebAuthnCredentials](#).

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request deletes the passkey credential with ID `gDHtiE8JgY8mZS_ABDl9sScfjgTG7TPwhlj4et9lxNlR1LTtnqwE_ObtR1hN_xU` from the user with access token `eyJra456defEXAMPLE`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DeleteWebAuthnCredential
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE",
  "CredentialId": "gDHtiE8JgY8mZS_ABDl9sScfjgTG7TPwhlj4et9lxNlR1LTtnqwE_ObtR1hN_xU"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
```



```
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

DescribeIdentityProvider

Given a user pool ID and identity provider (IdP) name, returns details about the IdP.

Request Syntax

```
{  
  "ProviderName": "string",  
  "UserPoolId": "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.

ProviderName

The name of the IdP that you want to describe.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\p{Z}]+`

Required: Yes

UserPoolId

The ID of the user pool that has the IdP that you want to describe..

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "IdentityProvider": {
    "AttributeMapping": {
      "string" : "string"
    },
    "CreationDate": number,
    "IdpIdentifiers": [ "string" ],
    "LastModifiedDate": number,
    "ProviderDetails": {
      "string" : "string"
    },
    "ProviderName": "string",
    "ProviderType": "string",
    "UserPoolId": "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.

IdentityProvider

The details of the requested IdP.

Type: [IdentityProviderType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request describes a Google IdP.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DescribeIdentityProvider
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ProviderName": "Google",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "IdentityProvider": {
    "AttributeMapping": {
      "email": "email",
      "username": "sub"
    },
    "CreationDate": 1635187122.265,
    "IdpIdentifiers": [],
    "LastModifiedDate": 1697051749.303,
    "ProviderDetails": {
      "attributes_url": "https://people.googleapis.com/v1/people/me?personFields=",
      "attributes_url_add_attributes": "true",
      "authorize_scopes": "email profile openid",

```

```
"authorize_url": "https://accounts.google.com/o/oauth2/v2/auth",
"client_id": "[client ID].apps.googleusercontent.com",
"client_secret": "[client secret]",
"oidc_issuer": "https://accounts.google.com",
"token_request_method": "POST",
"token_url": "https://www.googleapis.com/oauth2/v4/token"
},
"ProviderName": "Google",
"ProviderType": "Google",
"UserPoolId": "us-west-2_EXAMPLE"
}
}
```

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](#)

DescribeManagedLoginBranding

Given the ID of a managed login branding style, returns detailed information about the style.

Request Syntax

```
{  
  "ManagedLoginBrandingId": "string",  
  "ReturnMergedResources": boolean,  
  "UserPoolId": "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.

ManagedLoginBrandingId

The ID of the managed login branding style that you want to get more information about.

Type: String

Pattern: `^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[4][0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}$`

Required: Yes

ReturnMergedResources

When `true`, returns values for branding options that are unchanged from Amazon Cognito defaults. When `false` or when you omit this parameter, returns only values that you customized in your branding style.

Type: Boolean

Required: No

UserPoolId

The ID of the user pool that contains the managed login branding style that you want to get information about.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "ManagedLoginBranding": {
    "Assets": [
      {
        "Bytes": blob,
        "Category": "string",
        "ColorMode": "string",
        "Extension": "string",
        "ResourceId": "string"
      }
    ],
    "CreationDate": number,
    "LastModifiedDate": number,
    "ManagedLoginBrandingId": "string",
    "Settings": JSON value,
    "UseCognitoProvidedValues": boolean,
    "UserPoolId": "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.

ManagedLoginBranding

The details of the requested branding style.

Type: [ManagedLoginBrandingType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request returns the details of the managed login style with ID a1b2c3d4-5678-90ab-cdef-EXAMPLE11111.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.ca-central-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DescribeManagedLoginBranding
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ReturnMergedResources": false,
  "UserPoolId": "ca-central-1_EXAMPLE",
  "ManagedLoginBrandingId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
```

```
{
  "ManagedLoginBranding": {
    "Assets": [
      {
        "Bytes": "[encoded image file]",
        "Category": "PAGE_FOOTER_LOGO",
        "ColorMode": "LIGHT",
        "Extension": "JPEG"
      }
    ],
    "CreationDate": 1732667944.313,
    "LastModifiedDate": 1732668950.888,
    "ManagedLoginBrandingId": "ef1bb4d9-a28f-4dc6-94c6-49a605de6a6a",
    "Settings": {
      "categories": {
        "auth": {
          "authMethodOrder": [
            [
              {
                "display": "BUTTON",
                "type": "FEDERATED"
              },
              {
                "display": "INPUT",
                "type": "USERNAME_PASSWORD"
              }
            ]
          ],
          "federation": {
            "interfaceStyle": "BUTTON_LIST",
            "order": [
            ]
          }
        },
        "form": {
          "displayGraphics": true,
          "instructions": {
            "enabled": false
          },
          "languageSelector": {
            "enabled": false
          },
          "location": {
            "horizontal": "CENTER",
```

```
        "vertical": "CENTER"
      },
      "sessionTimerDisplay": "NONE"
    },
    "global": {
      "colorSchemeMode": "LIGHT",
      "pageFooter": {
        "enabled": true
      },
      "pageHeader": {
        "enabled": true
      },
      "spacingDensity": "REGULAR"
    },
    "signUp": {
      "acceptanceElements": [
        {
          "enforcement": "NONE",
          "textKey": "en"
        }
      ]
    }
  },
  "componentClasses": {
    "buttons": {
      "borderRadius": 8.0
    },
    "divider": {
      "darkMode": {
        "borderColor": "232b37ff"
      },
      "lightMode": {
        "borderColor": "ebbf0fff"
      }
    },
    "dropDown": {
      "borderRadius": 8.0,
      "darkMode": {
        "defaults": {
          "itemBackgroundColor": "192534ff"
        },
        "hover": {
          "itemBackgroundColor": "081120ff",
          "itemBorderColor": "5f6b7aff",
```

```
        "itemTextColor": "e9ebedff"
      },
      "match": {
        "itemBackgroundColor": "d1d5dbff",
        "itemTextColor": "89bdeeff"
      }
    },
    "lightMode": {
      "defaults": {
        "itemBackgroundColor": "ffffffff"
      },
      "hover": {
        "itemBackgroundColor": "f4f4f4ff",
        "itemBorderColor": "7d8998ff",
        "itemTextColor": "000716ff"
      },
      "match": {
        "itemBackgroundColor": "414d5cff",
        "itemTextColor": "0972d3ff"
      }
    }
  },
  "focusState": {
    "darkMode": {
      "borderColor": "539fe5ff"
    },
    "lightMode": {
      "borderColor": "0972d3ff"
    }
  },
  "idpButtons": {
    "icons": {
      "enabled": true
    }
  },
  "input": {
    "borderRadius": 8.0,
    "darkMode": {
      "defaults": {
        "backgroundColor": "0f1b2aff",
        "borderColor": "5f6b7aff"
      },
      "placeholderColor": "8d99a8ff"
    }
  },
```

```
        "lightMode": {
          "defaults": {
            "backgroundColor": "ffffffff",
            "borderColor": "7d8998ff"
          },
          "placeholderColor": "5f6b7aff"
        }
      },
      "inputDescription": {
        "darkMode": {
          "textColor": "8d99a8ff"
        },
        "lightMode": {
          "textColor": "5f6b7aff"
        }
      },
      "inputLabel": {
        "darkMode": {
          "textColor": "d1d5dbff"
        },
        "lightMode": {
          "textColor": "000716ff"
        }
      },
      "link": {
        "darkMode": {
          "defaults": {
            "textColor": "539fe5ff"
          },
          "hover": {
            "textColor": "89bdeeff"
          }
        },
        "lightMode": {
          "defaults": {
            "textColor": "0972d3ff"
          },
          "hover": {
            "textColor": "033160ff"
          }
        }
      },
      "optionControls": {
        "darkMode": {
```

```
        "defaults": {
            "backgroundColor": "0f1b2aff",
            "borderColor": "7d8998ff"
        },
        "selected": {
            "backgroundColor": "539fe5ff",
            "foregroundColor": "000716ff"
        }
    },
    "lightMode": {
        "defaults": {
            "backgroundColor": "ffffffff",
            "borderColor": "7d8998ff"
        },
        "selected": {
            "backgroundColor": "0972d3ff",
            "foregroundColor": "ffffffff"
        }
    }
},
"statusIndicator": {
    "darkMode": {
        "error": {
            "backgroundColor": "1a0000ff",
            "borderColor": "eb6f6fff",
            "indicatorColor": "eb6f6fff"
        },
        "pending": {
            "indicatorColor": "AAAAAAAA"
        },
        "success": {
            "backgroundColor": "001a02ff",
            "borderColor": "29ad32ff",
            "indicatorColor": "29ad32ff"
        },
        "warning": {
            "backgroundColor": "1d1906ff",
            "borderColor": "e0ca57ff",
            "indicatorColor": "e0ca57ff"
        }
    },
    "lightMode": {
        "error": {
            "backgroundColor": "fff7f7ff",
```

```

        "borderColor": "d91515ff",
        "indicatorColor": "d91515ff"
    },
    "pending": {
        "indicatorColor": "AAAAAAA"
    },
    "success": {
        "backgroundColor": "f2fcf3ff",
        "borderColor": "037f0cff",
        "indicatorColor": "037f0cff"
    },
    "warning": {
        "backgroundColor": "fffce9ff",
        "borderColor": "8d6605ff",
        "indicatorColor": "8d6605ff"
    }
}
},
"components": {
    "alert": {
        "borderRadius": 12.0,
        "darkMode": {
            "error": {
                "backgroundColor": "1a0000ff",
                "borderColor": "eb6f6fff"
            }
        },
        "lightMode": {
            "error": {
                "backgroundColor": "fff7f7ff",
                "borderColor": "d91515ff"
            }
        }
    },
    "favicon": {
        "enabledTypes": [
            "ICO",
            "SVG"
        ]
    },
    "form": {
        "backgroundImage": {
            "enabled": false

```



```
    },
    "borderRadius": 8.0,
    "darkMode": {
      "backgroundColor": "0f1b2aff",
      "borderColor": "424650ff"
    },
    "lightMode": {
      "backgroundColor": "ffffffff",
      "borderColor": "c6c6cdff"
    },
    "logo": {
      "enabled": false,
      "formInclusion": "IN",
      "location": "CENTER",
      "position": "TOP"
    }
  },
  "idpButton": {
    "custom": {
    },
    "standard": {
      "darkMode": {
        "active": {
          "backgroundColor": "354150ff",
          "borderColor": "89bdeeff",
          "textColor": "89bdeeff"
        },
        "defaults": {
          "backgroundColor": "0f1b2aff",
          "borderColor": "c6c6cdff",
          "textColor": "c6c6cdff"
        },
        "hover": {
          "backgroundColor": "192534ff",
          "borderColor": "89bdeeff",
          "textColor": "89bdeeff"
        }
      },
      "lightMode": {
        "active": {
          "backgroundColor": "d3e7f9ff",
          "borderColor": "033160ff",
          "textColor": "033160ff"
        },
      },
    }
  },
}
```

```
        "defaults": {
            "backgroundColor": "ffffffff",
            "borderColor": "424650ff",
            "textColor": "424650ff"
        },
        "hover": {
            "backgroundColor": "f2f8fdff",
            "borderColor": "033160ff",
            "textColor": "033160ff"
        }
    }
},
"pageBackground": {
    "darkMode": {
        "color": "0f1b2aff"
    },
    "image": {
        "enabled": true
    },
    "lightMode": {
        "color": "ffffffff"
    }
},
"pageFooter": {
    "backgroundImage": {
        "enabled": false
    },
    "darkMode": {
        "background": {
            "color": "0f141aff"
        },
        "borderColor": "424650ff"
    },
    "lightMode": {
        "background": {
            "color": "fafafaff"
        },
        "borderColor": "d5dbdbff"
    },
    "logo": {
        "enabled": true,
        "location": "CENTER"
    }
}
```

```
    },
    "pageHeader": {
      "backgroundImage": {
        "enabled": false
      },
      "darkMode": {
        "background": {
          "color": "0f141aff"
        },
        "borderColor": "424650ff"
      },
      "lightMode": {
        "background": {
          "color": "fafafaff"
        },
        "borderColor": "d5dbdbff"
      },
      "logo": {
        "enabled": false,
        "location": "START"
      }
    },
    "pageText": {
      "darkMode": {
        "bodyColor": "b6bec9ff",
        "descriptionColor": "b6bec9ff",
        "headingColor": "d1d5dbff"
      },
      "lightMode": {
        "bodyColor": "414d5cff",
        "descriptionColor": "414d5cff",
        "headingColor": "000716ff"
      }
    },
    "phoneNumberSelector": {
      "displayType": "TEXT"
    },
    "primaryButton": {
      "darkMode": {
        "active": {
          "backgroundColor": "539fe5ff",
          "textColor": "000716ff"
        },
        "defaults": {
```

```
        "backgroundColor": "539fe5ff",
        "textColor": "000716ff"
    },
    "disabled": {
        "backgroundColor": "ffffffff",
        "borderColor": "ffffffff"
    },
    "hover": {
        "backgroundColor": "89bdeeff",
        "textColor": "000716ff"
    }
},
"lightMode": {
    "active": {
        "backgroundColor": "033160ff",
        "textColor": "ffffffff"
    },
    "defaults": {
        "backgroundColor": "0972d3ff",
        "textColor": "ffffffff"
    },
    "disabled": {
        "backgroundColor": "ffffffff",
        "borderColor": "ffffffff"
    },
    "hover": {
        "backgroundColor": "033160ff",
        "textColor": "ffffffff"
    }
},
"secondaryButton": {
    "darkMode": {
        "active": {
            "backgroundColor": "354150ff",
            "borderColor": "89bdeeff",
            "textColor": "89bdeeff"
        },
        "defaults": {
            "backgroundColor": "0f1b2aff",
            "borderColor": "539fe5ff",
            "textColor": "539fe5ff"
        },
        "hover": {
```

```

        "backgroundColor": "192534ff",
        "borderColor": "89bdeeff",
        "textColor": "89bdeeff"
    },
    "lightMode": {
        "active": {
            "backgroundColor": "d3e7f9ff",
            "borderColor": "033160ff",
            "textColor": "033160ff"
        },
        "defaults": {
            "backgroundColor": "ffffffff",
            "borderColor": "0972d3ff",
            "textColor": "0972d3ff"
        },
        "hover": {
            "backgroundColor": "f2f8fdff",
            "borderColor": "033160ff",
            "textColor": "033160ff"
        }
    }
}
},
"UseCognitoProvidedValues": false,
"UserPoolId": "ca-central-1_EXAMPLE"
}
}

```

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](#)

DescribeManagedLoginBrandingByClient

Given the ID of a user pool app client, returns detailed information about the style assigned to the app client.

Request Syntax

```
{  
  "ClientId": "string",  
  "ReturnMergedResources": boolean,  
  "UserPoolId": "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.

ClientId

The app client that's assigned to the branding style that you want more information about.

Type: String

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

Pattern: `[\w+]`

Required: Yes

ReturnMergedResources

When `true`, returns values for branding options that are unchanged from Amazon Cognito defaults. When `false` or when you omit this parameter, returns only values that you customized in your branding style.

Type: Boolean

Required: No

UserPoolId

The ID of the user pool that contains the app client where you want more information about the managed login branding style.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w- ]+_[0-9a-zA-Z ]+`

Required: Yes

Response Syntax

```
{
  "ManagedLoginBranding": {
    "Assets": [
      {
        "Bytes": blob,
        "Category": "string",
        "ColorMode": "string",
        "Extension": "string",
        "ResourceId": "string"
      }
    ],
    "CreationDate": number,
    "LastModifiedDate": number,
    "ManagedLoginBrandingId": "string",
    "Settings": JSON value,
    "UseCognitoProvidedValues": boolean,
    "UserPoolId": "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.

ManagedLoginBranding

The details of the requested branding style.

Type: [ManagedLoginBrandingType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request returns managed login style details for the app client with ID `1example23456789`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.ca-central-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DescribeManagedLoginBrandingByClient
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ClientId": "1example23456789",
  "ReturnMergedResources": false,
  "UserPoolId": "ca-central-1_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "ManagedLoginBranding": {
    "Assets": [
      {
        "Bytes": "[encoded image file]",
        "Category": "PAGE_FOOTER_LOGO",
        "ColorMode": "LIGHT",
        "Extension": "JPEG"
      }
    ],
    "CreationDate": 1732667944.313,
    "LastModifiedDate": 1732668950.888,
    "ManagedLoginBrandingId": "ef1bb4d9-a28f-4dc6-94c6-49a605de6a6a",
    "Settings": {
      "categories": {
        "auth": {
          "authMethodOrder": [
            {
              "display": "BUTTON",
              "type": "FEDERATED"
            },
            {
              "display": "INPUT",
              "type": "USERNAME_PASSWORD"
            }
          ]
        },
        "federation": {
          "interfaceStyle": "BUTTON_LIST",
          "order": [
            ]
        }
      },
      "form": {
        "displayGraphics": true,

```

```
    "instructions": {
      "enabled": false
    },
    "languageSelector": {
      "enabled": false
    },
    "location": {
      "horizontal": "CENTER",
      "vertical": "CENTER"
    },
    "sessionTimerDisplay": "NONE"
  },
  "global": {
    "colorSchemeMode": "LIGHT",
    "pageFooter": {
      "enabled": true
    },
    "pageHeader": {
      "enabled": true
    },
    "spacingDensity": "REGULAR"
  },
  "signUp": {
    "acceptanceElements": [
      {
        "enforcement": "NONE",
        "textKey": "en"
      }
    ]
  }
},
"componentClasses": {
  "buttons": {
    "borderRadius": 8.0
  },
  "divider": {
    "darkMode": {
      "borderColor": "232b37ff"
    },
    "lightMode": {
      "borderColor": "ebbf0fff"
    }
  }
},
"dropDown": {
```

```
    "borderRadius": 8.0,
    "darkMode": {
      "defaults": {
        "itemBackgroundColor": "192534ff"
      },
      "hover": {
        "itemBackgroundColor": "081120ff",
        "itemBorderColor": "5f6b7aff",
        "itemTextColor": "e9ebedff"
      },
      "match": {
        "itemBackgroundColor": "d1d5dbff",
        "itemTextColor": "89bdeeff"
      }
    },
    "lightMode": {
      "defaults": {
        "itemBackgroundColor": "ffffffff"
      },
      "hover": {
        "itemBackgroundColor": "f4f4f4ff",
        "itemBorderColor": "7d8998ff",
        "itemTextColor": "000716ff"
      },
      "match": {
        "itemBackgroundColor": "414d5cff",
        "itemTextColor": "0972d3ff"
      }
    }
  },
  "focusState": {
    "darkMode": {
      "borderColor": "539fe5ff"
    },
    "lightMode": {
      "borderColor": "0972d3ff"
    }
  },
  "idpButtons": {
    "icons": {
      "enabled": true
    }
  },
  "input": {
```

```
    "borderRadius": 8.0,
    "darkMode": {
      "defaults": {
        "backgroundColor": "0f1b2aff",
        "borderColor": "5f6b7aff"
      },
      "placeholderColor": "8d99a8ff"
    },
    "lightMode": {
      "defaults": {
        "backgroundColor": "ffffffff",
        "borderColor": "7d8998ff"
      },
      "placeholderColor": "5f6b7aff"
    }
  },
  "inputDescription": {
    "darkMode": {
      "textColor": "8d99a8ff"
    },
    "lightMode": {
      "textColor": "5f6b7aff"
    }
  },
  "inputLabel": {
    "darkMode": {
      "textColor": "d1d5dbff"
    },
    "lightMode": {
      "textColor": "000716ff"
    }
  },
  "link": {
    "darkMode": {
      "defaults": {
        "textColor": "539fe5ff"
      },
      "hover": {
        "textColor": "89bdeeff"
      }
    },
    "lightMode": {
      "defaults": {
        "textColor": "0972d3ff"
      }
    }
  }
}
```

```
    },
    "hover": {
      "textColor": "033160ff"
    }
  }
},
"optionControls": {
  "darkMode": {
    "defaults": {
      "backgroundColor": "0f1b2aff",
      "borderColor": "7d8998ff"
    },
    "selected": {
      "backgroundColor": "539fe5ff",
      "foregroundColor": "000716ff"
    }
  },
  "lightMode": {
    "defaults": {
      "backgroundColor": "ffffffff",
      "borderColor": "7d8998ff"
    },
    "selected": {
      "backgroundColor": "0972d3ff",
      "foregroundColor": "ffffffff"
    }
  }
},
"statusIndicator": {
  "darkMode": {
    "error": {
      "backgroundColor": "1a0000ff",
      "borderColor": "eb6f6fff",
      "indicatorColor": "eb6f6fff"
    },
    "pending": {
      "indicatorColor": "AAAAAAA"
    },
    "success": {
      "backgroundColor": "001a02ff",
      "borderColor": "29ad32ff",
      "indicatorColor": "29ad32ff"
    },
    "warning": {
```

```

        "backgroundColor": "1d1906ff",
        "borderColor": "e0ca57ff",
        "indicatorColor": "e0ca57ff"
    },
    },
    "lightMode": {
        "error": {
            "backgroundColor": "fff7f7ff",
            "borderColor": "d91515ff",
            "indicatorColor": "d91515ff"
        },
        "pending": {
            "indicatorColor": "AAAAAAA"
        },
        "success": {
            "backgroundColor": "f2fcf3ff",
            "borderColor": "037f0cff",
            "indicatorColor": "037f0cff"
        },
        "warning": {
            "backgroundColor": "fffce9ff",
            "borderColor": "8d6605ff",
            "indicatorColor": "8d6605ff"
        }
    }
},
"components": {
    "alert": {
        "borderRadius": 12.0,
        "darkMode": {
            "error": {
                "backgroundColor": "1a0000ff",
                "borderColor": "eb6f6fff"
            }
        },
        "lightMode": {
            "error": {
                "backgroundColor": "fff7f7ff",
                "borderColor": "d91515ff"
            }
        }
    },
    "favicon": {

```



```
        "enabledTypes": [
            "IC0",
            "SVG"
        ],
    },
    "form": {
        "backgroundImage": {
            "enabled": false
        },
        "borderRadius": 8.0,
        "darkMode": {
            "backgroundColor": "0f1b2aff",
            "borderColor": "424650ff"
        },
        "lightMode": {
            "backgroundColor": "ffffffff",
            "borderColor": "c6c6cdff"
        },
        "logo": {
            "enabled": false,
            "formInclusion": "IN",
            "location": "CENTER",
            "position": "TOP"
        }
    },
    "idpButton": {
        "custom": {
        },
        "standard": {
            "darkMode": {
                "active": {
                    "backgroundColor": "354150ff",
                    "borderColor": "89bdeeff",
                    "textColor": "89bdeeff"
                },
                "defaults": {
                    "backgroundColor": "0f1b2aff",
                    "borderColor": "c6c6cdff",
                    "textColor": "c6c6cdff"
                }
            },
            "hover": {
                "backgroundColor": "192534ff",
                "borderColor": "89bdeeff",
                "textColor": "89bdeeff"
            }
        }
    }
}
```

```

        }
    },
    "lightMode": {
        "active": {
            "backgroundColor": "d3e7f9ff",
            "borderColor": "033160ff",
            "textColor": "033160ff"
        },
        "defaults": {
            "backgroundColor": "ffffffff",
            "borderColor": "424650ff",
            "textColor": "424650ff"
        },
        "hover": {
            "backgroundColor": "f2f8fdff",
            "borderColor": "033160ff",
            "textColor": "033160ff"
        }
    }
}
},
"pageBackground": {
    "darkMode": {
        "color": "0f1b2aff"
    },
    "image": {
        "enabled": true
    },
    "lightMode": {
        "color": "ffffffff"
    }
},
"pageFooter": {
    "backgroundImage": {
        "enabled": false
    },
    "darkMode": {
        "background": {
            "color": "0f141aff"
        },
        "borderColor": "424650ff"
    },
    "lightMode": {
        "background": {

```

```
        "color": "fafafaff"
      },
      "borderColor": "d5dbdbff"
    },
    "logo": {
      "enabled": true,
      "location": "CENTER"
    }
  },
  "pageHeader": {
    "backgroundImage": {
      "enabled": false
    },
    "darkMode": {
      "background": {
        "color": "0f141aff"
      },
      "borderColor": "424650ff"
    },
    "lightMode": {
      "background": {
        "color": "fafafaff"
      },
      "borderColor": "d5dbdbff"
    },
    "logo": {
      "enabled": false,
      "location": "START"
    }
  },
  "pageText": {
    "darkMode": {
      "bodyColor": "b6bec9ff",
      "descriptionColor": "b6bec9ff",
      "headingColor": "d1d5dbff"
    },
    "lightMode": {
      "bodyColor": "414d5cff",
      "descriptionColor": "414d5cff",
      "headingColor": "000716ff"
    }
  },
  "phoneNumberSelector": {
    "displayType": "TEXT"
```

```
    },
    "primaryButton": {
      "darkMode": {
        "active": {
          "backgroundColor": "539fe5ff",
          "textColor": "000716ff"
        },
        "defaults": {
          "backgroundColor": "539fe5ff",
          "textColor": "000716ff"
        },
        "disabled": {
          "backgroundColor": "ffffffff",
          "borderColor": "ffffffff"
        },
        "hover": {
          "backgroundColor": "89bdeeff",
          "textColor": "000716ff"
        }
      },
      "lightMode": {
        "active": {
          "backgroundColor": "033160ff",
          "textColor": "ffffffff"
        },
        "defaults": {
          "backgroundColor": "0972d3ff",
          "textColor": "ffffffff"
        },
        "disabled": {
          "backgroundColor": "ffffffff",
          "borderColor": "ffffffff"
        },
        "hover": {
          "backgroundColor": "033160ff",
          "textColor": "ffffffff"
        }
      }
    },
    "secondaryButton": {
      "darkMode": {
        "active": {
          "backgroundColor": "354150ff",
          "borderColor": "89bdeeff",
```

```

        "textColor": "89bdeeff"
    },
    "defaults": {
        "backgroundColor": "0f1b2aff",
        "borderColor": "539fe5ff",
        "textColor": "539fe5ff"
    },
    "hover": {
        "backgroundColor": "192534ff",
        "borderColor": "89bdeeff",
        "textColor": "89bdeeff"
    }
},
"lightMode": {
    "active": {
        "backgroundColor": "d3e7f9ff",
        "borderColor": "033160ff",
        "textColor": "033160ff"
    },
    "defaults": {
        "backgroundColor": "ffffffff",
        "borderColor": "0972d3ff",
        "textColor": "0972d3ff"
    },
    "hover": {
        "backgroundColor": "f2f8fdff",
        "borderColor": "033160ff",
        "textColor": "033160ff"
    }
}
}
},
"UseCognitoProvidedValues": false,
"UserPoolId": "ca-central-1_EXAMPLE"
}
}

```

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](#)

DescribeResourceServer

Describes a resource server. For more information about resource servers, see [Access control with resource servers](#).

Request Syntax

```
{  
  "Identifier": "string",  
  "UserPoolId": "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.

[Identifier](#)

A unique resource server identifier for the resource server. The identifier can be an API friendly name like `solar-system-data`. You can also set an API URL like `https://solar-system-data-api.example.com` as your identifier.

Amazon Cognito represents scopes in the access token in the format `$resource-server-identifier/$scope`. Longer scope-identifier strings increase the size of your access tokens.

Type: String

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

Pattern: `[\x21\x23-\x5B\x5D-\x7E]+`

Required: Yes

[UserPoolId](#)

The ID of the user pool that hosts the resource server.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "ResourceServer": {
    "Identifier": "string",
    "Name": "string",
    "Scopes": [
      {
        "ScopeDescription": "string",
        "ScopeName": "string"
      }
    ],
    "UserPoolId": "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.

ResourceServer

The details of the requested resource server.

Type: [ResourceServerType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request returns details about the resource server `myapi.example.com` in user pool `us-west-2_EXAMPLE`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DescribeResourceServer
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "Identifier": "myapi.example.com",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "ResourceServer": {
    "Identifier": "myapi.example.com",
    "Name": "Example API with custom access control scopes",
    "Scopes": [
      {
        "ScopeDescription": "International customers",
        "ScopeName": "international.read"
      },

```

```
{
  "ScopeDescription": "Domestic customers",
  "ScopeName": "domestic.read"
},
"UserPoolId": "us-west-2_EXAMPLE"
}
```

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](#)

DescribeRiskConfiguration

Given an app client or user pool ID where threat protection is configured, describes the risk configuration. This operation returns details about adaptive authentication, compromised credentials, and IP-address allow- and denylists. For more information about threat protection, see [Threat protection](#).

Request Syntax

```
{  
  "ClientId": "string",  
  "UserPoolId": "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.

[ClientId](#)

The ID of the app client with the risk configuration that you want to inspect. You can apply default risk configuration at the user pool level and further customize it from user pool defaults at the app-client level. Specify `ClientId` to inspect client-level configuration, or `UserPoolId` to inspect pool-level configuration.

Type: String

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

Pattern: `[\w+]`+

Required: No

[UserPoolId](#)

The ID of the user pool with the risk configuration that you want to inspect. You can apply default risk configuration at the user pool level and further customize it from user pool defaults at the app-client level. Specify `ClientId` to inspect client-level configuration, or `UserPoolId` to inspect pool-level configuration.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "RiskConfiguration": {
    "AccountTakeoverRiskConfiguration": {
      "Actions": {
        "HighAction": {
          "EventAction": "string",
          "Notify": boolean
        },
        "LowAction": {
          "EventAction": "string",
          "Notify": boolean
        },
        "MediumAction": {
          "EventAction": "string",
          "Notify": boolean
        }
      },
      "NotifyConfiguration": {
        "BlockEmail": {
          "HtmlBody": "string",
          "Subject": "string",
          "TextBody": "string"
        },
        "From": "string",
        "MfaEmail": {
          "HtmlBody": "string",
          "Subject": "string",
          "TextBody": "string"
        },
        "NoActionEmail": {
          "HtmlBody": "string",
          "Subject": "string",
          "TextBody": "string"
        }
      }
    }
  }
}
```

```
    },
    "ReplyTo": "string",
    "SourceArn": "string"
  }
},
"ClientId": "string",
"CompromisedCredentialsRiskConfiguration": {
  "Actions": {
    "EventAction": "string"
  },
  "EventFilter": [ "string" ]
},
"LastModifiedDate": number,
"RiskExceptionConfiguration": {
  "BlockedIPRangeList": [ "string" ],
  "SkippedIPRangeList": [ "string" ]
},
"UserPoolId": "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.

RiskConfiguration

The details of the requested risk configuration.

Type: [RiskConfigurationType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserPoolAddOnNotEnabledException

This exception is thrown when user pool add-ons aren't enabled.

HTTP Status Code: 400

Examples

Example

The following example request describes the threat protection configuration of the app client with ID 1example23456789.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DescribeRiskConfiguration
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ClientId": "1example23456789",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "RiskConfiguration": {
    "AccountTakeoverRiskConfiguration": {
      "Actions": {
        "HighAction": {
```



```

        "EventAction": "MFA_REQUIRED",
        "Notify": true
    },
    "LowAction": {
        "EventAction": "NO_ACTION",
        "Notify": true
    },
    "MediumAction": {
        "EventAction": "MFA_IF_CONFIGURED",
        "Notify": true
    }
},
"NotifyConfiguration": {
    "BlockEmail": {
        "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML email context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We blocked an unrecognized sign-in to your account with this information:\n<ul>\n<li>Time: {login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city}, {country}</li>\n</ul>\nIf this sign-in was not by you, you should change your password and notify us by clicking on <a href={one-click-link-invalid}>this link</a>\nIf this sign-in was by you, you can follow <a href={one-click-link-valid}>this link</a> to let us know</pre>\n</body>\n</html>",
        "Subject": "Blocked sign-in attempt",
        "TextBody": "We blocked an unrecognized sign-in to your account with this information:\nTime: {login-time}\nDevice: {device-name}\nLocation: {city}, {country}\nIf this sign-in was not by you, you should change your password and notify us by clicking on {one-click-link-invalid}\nIf this sign-in was by you, you can follow {one-click-link-valid} to let us know"
    },
    "From": "admin@example.com",
    "MfaEmail": {
        "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML email context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We required you to use multi-factor authentication for the following sign-in attempt:\n<ul>\n<li>Time: {login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city}, {country}</li>\n</ul>\nIf this sign-in was not by you, you should change your password and notify us by clicking on <a href={one-click-link-invalid}>this link</a>\nIf this sign-in was by you, you can follow <a href={one-click-link-valid}>this link</a> to let us know</pre>\n</body>\n</html>",
        "Subject": "New sign-in attempt",
        "TextBody": "We required you to use multi-factor authentication for the following sign-in attempt:\nTime: {login-time}\nDevice: {device-name}\nLocation: {city}, {country}\nIf this sign-in was not by you, you should change your password and

```

```

    notify us by clicking on {one-click-link-invalid}\nIf this sign-in was by you, you can
    follow {one-click-link-valid} to let us know"
    },
    "NoActionEmail": {
      "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML email
context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We observed an
unrecognized sign-in to your account with this information:\n<ul>\n<li>Time: {login-
time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city}, {country}</li>\n</
ul>\nIf this sign-in was not by you, you should change your password and notify us by
clicking on <a href={one-click-link-invalid}>this link</a>\nIf this sign-in was by
you, you can follow <a href={one-click-link-valid}>this link</a> to let us know</pre>
\n</body>\n</html>",
      "Subject": "New sign-in attempt",
      "TextBody": "We observed an unrecognized sign-in to your account
with this information:\nTime: {login-time}\nDevice: {device-name}\nLocation: {city},
{country}\nIf this sign-in was not by you, you should change your password and notify
us by clicking on {one-click-link-invalid}\nIf this sign-in was by you, you can follow
{one-click-link-valid} to let us know"
    },
    "ReplyTo": "admin@example.com",
    "SourceArn": "arn:aws:ses:us-east-1:123456789012:identity/
admin@example.com"
  }
},
"ClientId": "1example23456789",
"CompromisedCredentialsRiskConfiguration": {
  "Actions": {
    "EventAction": "BLOCK"
  },
  "EventFilter": [
    "PASSWORD_CHANGE",
    "SIGN_UP",
    "SIGN_IN"
  ]
},
"UserPoolId": "us-west-2_EXAMPLE"
}
}

```

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](#)

DescribeTerms

Returns details for the requested terms documents ID. For more information, see [Terms documents](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "TermsId": "string",  
  "UserPoolId": "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.

[TermsId](#)

The ID of the terms documents that you want to describe.

Type: String

Pattern: `^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[4][0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}$`

Required: Yes

UserPoolId

The ID of the user pool that contains the terms documents that you want to describe.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "Terms": {
    "ClientId": "string",
    "CreationDate": number,
    "Enforcement": "string",
    "LastModifiedDate": number,
    "Links": {
      "string" : "string"
    },
    "TermsId": "string",
    "TermsName": "string",
    "TermsSource": "string",
    "UserPoolId": "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.

Terms

A summary of the requested terms documents. Includes a unique identifier for later changes to the terms documents.

Type: [TermsType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example operation retrieves details for a specific terms document using its TermsId.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DescribeTerms
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "TermsId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "UserPoolId": "us-east-1_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
```

Connection: keep-alive

```
{
  "Terms": {
    "ClientId": "1example23456789",
    "CreationDate": 1755794156.892,
    "Enforcement": "NONE",
    "LastModifiedDate": 1755794201.567,
    "Links": {
      "cognito:default": "https://example.com/privacy/",
      "cognito:french": "https://example.com/fr/privacy/",
      "cognito:portuguese-brazil": "https://example.com/pt/privacy/"
    },
    "TermsId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "TermsName": "privacy-policy",
    "TermsSource": "LINK",
    "UserPoolId": "us-east-1_EXAMPLE"
  }
}
```

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](#)

DescribeUserImportJob

Describes a user import job. For more information about user CSV import, see [Importing users from a CSV file](#).

Request Syntax

```
{  
  "JobId": "string",  
  "UserPoolId": "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.

[JobId](#)

The Id of the user import job that you want to describe.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: import-[0-9a-zA-Z-]+

Required: Yes

[UserPoolId](#)

The ID of the user pool that's associated with the import job.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: [\w-]+_[0-9a-zA-Z-]+

Required: Yes

Response Syntax

```
{
  "UserImportJob": {
    "CloudWatchLogsRoleArn": "string",
    "CompletionDate": number,
    "CompletionMessage": "string",
    "CreationDate": number,
    "FailedUsers": number,
    "ImportedUsers": number,
    "JobId": "string",
    "JobName": "string",
    "PreSignedUrl": "string",
    "SkippedUsers": number,
    "StartDate": number,
    "Status": "string",
    "UserPoolId": "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.

UserImportJob

The details of the user import job. Includes logging destination, status, and the Amazon S3 pre-signed URL for CSV upload.

Type: [UserImportJobType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request describes the user import operation with the ID `import-mAgUtd8PMm`. In this example, the job ran after creation and successfully imported 99 users.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DescribeUserImportJob
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "JobId": "import-mAgUtd8PMm",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "UserImportJob": {
    "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/example-cloudwatch-logs-
role",
    "CreationDate": 1735241621.022,
    "FailedUsers": 1,
    "ImportedUsers": 99,
    "JobId": "import-mAgUtd8PMm",
    "JobName": "Customer import",
```

```
"PreSignedUrl": "https://aws-cognito-idp-user-import-pdx.s3.us-west-2.amazonaws.com/123456789012/us-west-2_EXAMPLE/import-mAgUtd8PMm?X-Amz-Security-Token=[token]&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20241226T193341Z&X-Amz-SignedHeaders=host%3Bx-amz-server-side-encryption&X-Amz-Expires=899&X-Amz-Credential=[credential]&X-Amz-Signature=[signature]",
  "SkippedUsers": 0,
  "Status": "Succeeded",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

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](#)

DescribeUserPool

Given a user pool ID, returns configuration information. This operation is useful when you want to inspect an existing user pool and programmatically replicate the configuration to another user pool.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "UserPoolId": "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.

UserPoolId

The ID of the user pool you want to describe.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "UserPool": {
    "AccountRecoverySetting": {
      "RecoveryMechanisms": [
        {
          "Name": "string",
          "Priority": number
        }
      ]
    },
    "AdminCreateUserConfig": {
      "AllowAdminCreateUserOnly": boolean,
      "InviteMessageTemplate": {
        "EmailMessage": "string",
        "EmailSubject": "string",
        "SMSMessage": "string"
      },
      "UnusedAccountValidityDays": number
    },
    "AliasAttributes": [ "string" ],
    "Arn": "string",
    "AutoVerifiedAttributes": [ "string" ],
    "CreationDate": number,
    "CustomDomain": "string",
    "DeletionProtection": "string",
    "DeviceConfiguration": {
      "ChallengeRequiredOnNewDevice": boolean,
      "DeviceOnlyRememberedOnUserPrompt": boolean
    },
    "Domain": "string",
    "EmailConfiguration": {
      "ConfigurationSet": "string",
      "EmailSendingAccount": "string",
      "From": "string",
      "ReplyToEmailAddress": "string",
      "SourceArn": "string"
    },
    "EmailConfigurationFailure": "string",
    "EmailVerificationMessage": "string",
    "EmailVerificationSubject": "string",
    "EstimatedNumberOfUsers": number,
```

```
"Id": "string",
"LambdaConfig": {
  "CreateAuthChallenge": "string",
  "CustomEmailSender": {
    "LambdaArn": "string",
    "LambdaVersion": "string"
  },
  "CustomMessage": "string",
  "CustomSMSSender": {
    "LambdaArn": "string",
    "LambdaVersion": "string"
  },
  "DefineAuthChallenge": "string",
  "InboundFederation": {
    "LambdaArn": "string",
    "LambdaVersion": "string"
  },
  "KMSKeyID": "string",
  "PostAuthentication": "string",
  "PostConfirmation": "string",
  "PreAuthentication": "string",
  "PreSignUp": "string",
  "PreTokenGeneration": "string",
  "PreTokenGenerationConfig": {
    "LambdaArn": "string",
    "LambdaVersion": "string"
  },
  "UserMigration": "string",
  "VerifyAuthChallengeResponse": "string"
},
"LastModifiedDate": number,
"MfaConfiguration": "string",
"Name": "string",
"Policies": {
  "PasswordPolicy": {
    "MinimumLength": number,
    "PasswordHistorySize": number,
    "RequireLowercase": boolean,
    "RequireNumbers": boolean,
    "RequireSymbols": boolean,
    "RequireUppercase": boolean,
    "TemporaryPasswordValidityDays": number
  },
  "SignInPolicy": {
```



```

    "AllowedFirstAuthFactors": [ "string" ]
  },
  "SchemaAttributes": [
    {
      "AttributeDataType": "string",
      "DeveloperOnlyAttribute": boolean,
      "Mutable": boolean,
      "Name": "string",
      "NumberAttributeConstraints": {
        "MaxValue": "string",
        "MinValue": "string"
      },
      "Required": boolean,
      "StringAttributeConstraints": {
        "MaxLength": "string",
        "MinLength": "string"
      }
    }
  ],
  "SmsAuthenticationMessage": "string",
  "SmsConfiguration": {
    "ExternalId": "string",
    "SnsCallerArn": "string",
    "SnsRegion": "string"
  },
  "SmsConfigurationFailure": "string",
  "SmsVerificationMessage": "string",
  "Status": "string",
  "UserAttributeUpdateSettings": {
    "AttributesRequireVerificationBeforeUpdate": [ "string" ]
  },
  "UsernameAttributes": [ "string" ],
  "UsernameConfiguration": {
    "CaseSensitive": boolean
  },
  "UserPoolAddOns": {
    "AdvancedSecurityAdditionalFlows": {
      "CustomAuthMode": "string"
    },
    "AdvancedSecurityMode": "string"
  },
  "UserPoolTags": {
    "string" : "string"
  }

```

```
    },  
    "UserPoolTier": "string",  
    "VerificationMessageTemplate": {  
        "DefaultEmailOption": "string",  
        "EmailMessage": "string",  
        "EmailMessageByLink": "string",  
        "EmailSubject": "string",  
        "EmailSubjectByLink": "string",  
        "SmsMessage": "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.

UserPool

The details of the requested user pool.

Type: [UserPoolType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserPoolTaggingException

This exception is thrown when a user pool tag can't be set or updated.

HTTP Status Code: 400

Examples

Example

The following example request describes the user pool `us-east-1_EXAMPLE`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-east-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DescribeUserPool
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-east-1_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "UserPool": {
    "AccountRecoverySetting": {
      "RecoveryMechanisms": [
        {
          "Name": "verified_email",
          "Priority": 1
        }
      ]
    },
    "AdminCreateUserConfig": {
      "AllowAdminCreateUserOnly": false,
      "InviteMessageTemplate": {
```

```

        "EmailMessage": "Your username is {username} and temporary password is
{####}.",
        "EmailSubject": "Your sign-in information",
        "SMSMessage": "Your username is {username} and temporary password is
{####}."
    },
    "UnusedAccountValidityDays": 7
},
"AliasAttributes": [
    "email"
],
"Arn": "arn:aws:cognito-idp:us-east-1:123456789012:userpool/us-east-1_EXAMPLE",
"AutoVerifiedAttributes": [
    "email"
],
"CreationDate": 1689721665.239,
"DeletionProtection": "ACTIVE",
"DeviceConfiguration": {
    "ChallengeRequiredOnNewDevice": true,
    "DeviceOnlyRememberedOnUserPrompt": true
},
"EmailConfiguration": {
    "ConfigurationSet": "my-test-ses-configuration-set",
    "EmailSendingAccount": "DEVELOPER",
    "From": "support@example.com",
    "ReplyToEmailAddress": "support@example.com",
    "SourceArn": "arn:aws:ses:us-east-1:123456789012:identity/
support@example.com"
},
"EmailVerificationMessage": "Your verification code is {####}.",
"EmailVerificationSubject": "Verify your email address",
"EstimatedNumberOfUsers": 0,
"Id": "us-east-1_EXAMPLE",
"LambdaConfig": {
    "CustomEmailSender": {
        "LambdaArn": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
        "LambdaVersion": "V1_0"
    },
    "CustomMessage": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
    "CustomSMSSender": {
        "LambdaArn": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",

```

```

        "LambdaVersion": "V1_0"
    },
    "DefineAuthChallenge": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
    "KMSKeyID": "arn:aws:kms:us-
east-1:767671399759:key/4d43904c-8edf-4bb4-9fca-fb1a80e41cbe",
    "PostAuthentication": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
    "PostConfirmation": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
    "PreAuthentication": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
    "PreSignUp": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
    "PreTokenGeneration": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
    "UserMigration": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
    "VerifyAuthChallengeResponse": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
    "InboundFederation": {
        "LambdaArn": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
        "LambdaVersion": "V1_0"
    }
},
"LastModifiedDate": 1689721665.239,
"MfaConfiguration": "OPTIONAL",
"Name": "my-test-user-pool",
"Policies": {
    "PasswordPolicy": {
        "MinimumLength": 6,
        "RequireLowercase": true,
        "RequireNumbers": true,
        "RequireSymbols": true,
        "RequireUppercase": true,
        "TemporaryPasswordValidityDays": 7
    }
},
"SchemaAttributes": [
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": false,
        "Name": "sub",

```

```
        "Required": true,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "1"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "name",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "given_name",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "family_name",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "middle_name",
```

```
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "nickname",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "preferred_username",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "profile",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "picture",
```



```
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "website",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "email",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    },
    {
        "AttributeDataType": "Boolean",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "email_verified",
        "Required": false
    },
    {
        "AttributeDataType": "String",
        "DeveloperOnlyAttribute": false,
        "Mutable": true,
        "Name": "gender",
        "Required": false,
        "StringAttributeConstraints": {
            "MaxLength": "2048",
            "MinLength": "0"
        }
    }
}
```

```
    }
  },
  {
    "AttributeDataType": "String",
    "DeveloperOnlyAttribute": false,
    "Mutable": true,
    "Name": "birthdate",
    "Required": false,
    "StringAttributeConstraints": {
      "MaxLength": "10",
      "MinLength": "10"
    }
  },
  {
    "AttributeDataType": "String",
    "DeveloperOnlyAttribute": false,
    "Mutable": true,
    "Name": "zoneinfo",
    "Required": false,
    "StringAttributeConstraints": {
      "MaxLength": "2048",
      "MinLength": "0"
    }
  },
  {
    "AttributeDataType": "String",
    "DeveloperOnlyAttribute": false,
    "Mutable": true,
    "Name": "locale",
    "Required": false,
    "StringAttributeConstraints": {
      "MaxLength": "2048",
      "MinLength": "0"
    }
  },
  {
    "AttributeDataType": "String",
    "DeveloperOnlyAttribute": false,
    "Mutable": true,
    "Name": "phone_number",
    "Required": false,
    "StringAttributeConstraints": {
      "MaxLength": "2048",
      "MinLength": "0"
    }
  }
}
```

```

    }
  },
  {
    "AttributeDataType": "Boolean",
    "DeveloperOnlyAttribute": false,
    "Mutable": true,
    "Name": "phone_number_verify",
    "Required": false
  },
  {
    "AttributeDataType": "String",
    "DeveloperOnlyAttribute": false,
    "Mutable": true,
    "Name": "address",
    "Required": false,
    "StringAttributeConstraints": {
      "MaxLength": "2048",
      "MinLength": "0"
    }
  },
  {
    "AttributeDataType": "Number",
    "DeveloperOnlyAttribute": false,
    "Mutable": true,
    "Name": "updated_at",
    "NumberAttributeConstraints": {
      "MinValue": "0"
    },
    "Required": false
  },
  {
    "AttributeDataType": "Number",
    "DeveloperOnlyAttribute": true,
    "Mutable": true,
    "Name": "dev:custom:mydev",
    "NumberAttributeConstraints": {
      "MaxValue": "99",
      "MinValue": "1"
    },
    "Required": false
  }
],
"SmsAuthenticationMessage": "Your verification code is {####}.",
"SmsConfiguration": {

```

```

        "ExternalId": "my-role-external-id",
        "SnsCallerArn": "arn:aws:iam::123456789012:role/service-role/test-cognito-
SMS-Role",
        "SnsRegion": "us-east-1"
    },
    "SmsVerificationMessage": "Your verification code is {####}.",
    "UserAttributeUpdateSettings": {
        "AttributesRequireVerificationBeforeUpdate": [
            "email"
        ]
    },
    "UserPoolAddOns": {
        "AdvancedSecurityMode": "OFF"
    },
    "UserPoolTags": {
        "my-test-tag-key": "my-test-tag-value"
    },
    "UserPoolTier": "ESSENTIALS",
    "UsernameConfiguration": {
        "CaseSensitive": true
    },
    "VerificationMessageTemplate": {
        "DefaultEmailOption": "CONFIRM_WITH_CODE",
        "EmailMessage": "Your confirmation code is {####}",
        "EmailMessageByLink": "Choose this link to {##verify your email##}",
        "EmailSubject": "Here is your confirmation code",
        "EmailSubjectByLink": "Here is your confirmation link",
        "SmsMessage": "Your confirmation code is {####}"
    }
}

```

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](#)

DescribeUserPoolClient

Given an app client ID, returns configuration information. This operation is useful when you want to inspect an existing app client and programmatically replicate the configuration to another app client. For more information about app clients, see [App clients](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "ClientId": "string",  
  "UserPoolId": "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.

[ClientId](#)

The ID of the app client that you want to describe.

Type: String

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

Pattern: `[\w+]`

Required: Yes

UserPoolId

The ID of the user pool that contains the app client you want to describe.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "UserPoolClient": {
    "AccessTokenValidity": number,
    "AllowedOAuthFlows": [ "string" ],
    "AllowedOAuthFlowsUserPoolClient": boolean,
    "AllowedOAuthScopes": [ "string" ],
    "AnalyticsConfiguration": {
      "ApplicationArn": "string",
      "ApplicationId": "string",
      "ExternalId": "string",
      "RoleArn": "string",
      "UserDataShared": boolean
    },
    "AuthSessionValidity": number,
    "CallbackURLs": [ "string" ],
    "ClientId": "string",
    "ClientName": "string",
    "ClientSecret": "string",
    "CreationDate": number,
    "DefaultRedirectURI": "string",
    "EnablePropagateAdditionalUserContextData": boolean,
    "EnableTokenRevocation": boolean,
    "ExplicitAuthFlows": [ "string" ],
    "IdTokenValidity": number,
    "LastModifiedDate": number,
    "LogoutURLs": [ "string" ],
    "PreventUserExistenceErrors": "string",
```

```
"ReadAttributes": [ "string" ],
"RefreshTokenRotation": {
  "Feature": "string",
  "RetryGracePeriodSeconds": number
},
"RefreshTokenValidity": number,
"SupportedIdentityProviders": [ "string" ],
"TokenValidityUnits": {
  "AccessToken": "string",
  "IdToken": "string",
  "RefreshToken": "string"
},
"UserPoolId": "string",
"WriteAttributes": [ "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.

UserPoolClient

The details of the request app client.

Type: [UserPoolClientType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request describes the app client with the ID 1example23456789.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-east-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DescribeUserPoolClient
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ClientId": "1example23456789",
  "UserPoolId": "us-east-1_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "UserPoolClient": {
    "AccessTokenValidity": 6,
    "AllowedOAuthFlows": [
      "code"
    ],
    "AllowedOAuthFlowsUserPoolClient": true,
    "AllowedOAuthScopes": [
      "aws.cognito.signin.user.admin",
      "openid"
    ],
    "AnalyticsConfiguration": {
```

```
    "ApplicationId": "d70b2ba36a8c4dc5a04a0451a31a1e12",
    "ExternalId": "my-external-id",
    "RoleArn": "arn:aws:iam::123456789012:role/test-cognitouserpool-role",
    "UserDataShared": true
  },
  "AuthSessionValidity": 3,
  "CallbackURLs": [
    "https://example.com",
    "http://localhost",
    "myapp://example"
  ],
  "ClientId": "1example23456789",
  "ClientName": "my-test-app-client",
  "ClientSecret": "13ka4h7u28d9oo44tqpq9djqsfvhvu8rk4d2ighvpu0k8fj1c2r9",
  "CreationDate": 1689885426.107,
  "DefaultRedirectURI": "https://example.com",
  "EnablePropagateAdditionalUserContextData": false,
  "EnableTokenRevocation": true,
  "ExplicitAuthFlows": [
    "ALLOW_USER_AUTH",
    "ALLOW_USER_PASSWORD_AUTH",
    "ALLOW_ADMIN_USER_PASSWORD_AUTH",
    "ALLOW_REFRESH_TOKEN_AUTH"
  ],
  "IdTokenValidity": 6,
  "LastModifiedDate": 1689885426.107,
  "LogoutURLs": [
    "https://example.com/logout"
  ],
  "PreventUserExistenceErrors": "ENABLED",
  "ReadAttributes": [
    "address",
    "preferred_username",
    "email"
  ],
  "RefreshTokenValidity": 6,
  "SupportedIdentityProviders": [
    "SignInWithApple",
    "MySSO"
  ],
  "TokenValidityUnits": {
    "AccessToken": "hours",
    "IdToken": "minutes",
    "RefreshToken": "days"
  }
```

```
    },  
    "UserPoolId": "us-east-1_EXAMPLE",  
    "WriteAttributes": [  
        "family_name",  
        "email"  
    ]  
}  
}
```

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](#)

DescribeUserPoolDomain

Given a user pool domain name, returns information about the domain configuration.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "Domain": "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.

Domain

The domain that you want to describe. For custom domains, this is the fully-qualified domain name, such as `auth.example.com`. For Amazon Cognito prefix domains, this is the prefix alone, such as `auth`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 63.

Pattern: `^[a-z0-9](?:[a-z0-9\-\]{0,61}[a-z0-9])?$`

Required: Yes

Response Syntax

```
{
  "DomainDescription": {
    "AWSAccountId": "string",
    "CloudFrontDistribution": "string",
    "CustomDomainConfig": {
      "CertificateArn": "string"
    },
    "Domain": "string",
    "ManagedLoginVersion": number,
    "S3Bucket": "string",
    "Status": "string",
    "UserPoolId": "string",
    "Version": "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.

DomainDescription

The details of the requested user pool domain.

Type: [DomainDescriptionType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

Examples

Example

The following example request describes the custom domain `auth.example.com` for the user pool `us-west-2_EXAMPLE`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
```

```
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.DescribeUserPoolDomain
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "Domain": "auth.example.com"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "DomainDescription": {
    "AWSAccountId": "123456789012",
    "CloudFrontDistribution": "example.cloudfront.net",
    "CustomDomainConfig": {
      "CertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
    "Domain": "auth.example.com",
    "ManagedLoginVersion": 2,
    "S3Bucket": "aws-cognito-prod-pdx-assets",
    "Status": "ACTIVE",
    "UserPoolId": "us-west-2_EXAMPLE",
    "Version": "20241127003837"
  }
}
```

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](#)

ForgetDevice

Given a device key, deletes a remembered device as the currently signed-in user. For more information about device authentication, see [Working with user devices in your user pool](#).

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{
  "AccessToken": "string",
  "DeviceKey": "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.

AccessToken

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: No

DeviceKey

The unique identifier, or device key, of the device that the user wants to forget.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w- ]+_[0-9a-f- ]+`

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](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request .

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ForgetDevice
```

```
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE",
  "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
}
```

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](#)

ForgotPassword

Sends a password-reset confirmation code to the email address or phone number of the requested username. The message delivery method is determined by the user's available attributes and the `AccountRecoverySetting` configuration of the user pool.

For the `Username` parameter, you can use the username or an email, phone, or preferred username alias.

Amazon Cognito sends the code with the delivery method specified by your user pool [CreateUserPool:AccountRecoverySetting](#) configuration. For more information, see [Recovering user accounts](#) in the *Amazon Cognito Developer Guide*. Users must submit the code in a [ConfirmForgotPassword](#) request.

If neither a verified phone number nor a verified email exists, Amazon Cognito responds with an `InvalidParameterException` error. If your app client has a client secret and you don't provide a `SECRET_HASH` parameter, this API returns `NotAuthorizedException`.

To use this API operation, your user pool must have self-service account recovery options set in [AccountRecoverySettingType](#) and the requested user must be eligible for an available account recovery option. Use [AdminSetUserPassword](#) if you manage passwords as an administrator.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Request Syntax

```
{
  "AnalyticsMetadata": {
    "AnalyticsEndpointId": "string"
  },
  "ClientId": "string",
  "ClientMetadata": {
    "string" : "string"
  },
  "SecretHash": "string",
  "UserContextData": {
    "EncodedData": "string",
    "IpAddress": "string"
  },
  "Username": "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.

[AnalyticsMetadata](#)

Information that supports analytics outcomes with Amazon Pinpoint, including the user's endpoint ID. The endpoint ID is a destination for Amazon Pinpoint push notifications, for example a device identifier, email address, or phone number.

Type: [AnalyticsMetadataType](#) object

Required: No

ClientId

The ID of the user pool app client associated with the current signed-in user.

Type: String

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

Pattern: `[\w+]`

Required: Yes

ClientMetadata

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

SecretHash

A keyed-hash message authentication code (HMAC) calculated using the secret key of a user pool client and username plus the client ID in the message. For more information about SecretHash, see [Computing secret hash values](#).

Type: String

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

Pattern: `[\w+=/+]`

Required: No

UserContextData

Contextual data about your user session like the device fingerprint, IP address, or location. Amazon Cognito threat protection evaluates the risk of an authentication event based on the context that your app generates and passes to Amazon Cognito when it makes API requests.

For more information, see [Collecting data for threat protection in applications](#).

Type: [UserContextDataType](#) object

Required: No

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]`

Required: Yes

Response Syntax

```
{
  "CodeDeliveryDetails": {
    "AttributeName": "string",
    "DeliveryMedium": "string",
    "Destination": "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.

[CodeDeliveryDetails](#)

Information about the phone number or email address that Amazon Cognito sent the password-recovery code to.

Type: [CodeDeliveryDetailsType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

CodeDeliveryFailureException

This exception is thrown when a verification code fails to deliver successfully.

message

The message sent when a verification code fails to deliver successfully.

HTTP Status Code: 400

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request requests a forgot-password code for the user "testuser". Amazon Cognito responds with confirmation that it has delivered the code in an email message.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ForgotPassword
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ClientId": "lexample23456789",
  "Username": "testuser"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
```

```
"CodeDeliveryDetails": {  
  "AttributeName": "email",  
  "DeliveryMedium": "EMAIL",  
  "Destination": "a***@e***"  
}
```

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](#)

GetCSVHeader

Given a user pool ID, generates a comma-separated value (CSV) list populated with available user attributes in the user pool. This list is the header for the CSV file that determines the users in a user import job. Save the content of CSVHeader in the response as a .csv file and populate it with the usernames and attributes of users that you want to import. For more information about CSV user import, see [Importing users from a CSV file](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "UserPoolId": "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.

[UserPoolId](#)

The ID of the user pool that you want to import users into.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "CSVHeader": [ "string" ],
  "UserPoolId": "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.

CSVHeader

A comma-separated list of attributes from your user pool. Save this output to a .csv file and populate it with the attributes of the users that you want to import.

Type: Array of strings

Length Constraints: Minimum length of 0. Maximum length of 131072.

UserPoolId

The ID of the requested user pool.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request retrieves the attributes from a user pool in CSV format for an import job.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.GetCSVHeader
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "CSVHeader": [
    "name",
    "given_name",
```

```
    "family_name",
    "middle_name",
    "nickname",
    "preferred_username",
    "profile",
    "picture",
    "website",
    "email",
    "email_verified",
    "gender",
    "birthdate",
    "zoneinfo",
    "locale",
    "phone_number",
    "phone_number_verified",
    "address",
    "updated_at",
    "custom:costcenter",
    "custom:accesstoken",
    "custom:idtoken",
    "dev:custom:bandwidth",
    "cognito:mfa_enabled",
    "cognito:username"
  ],
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

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](#)

GetDevice

Given a device key, returns information about a remembered device for the current user. For more information about device authentication, see [Working with user devices in your user pool](#).

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{
  "AccessToken": "string",
  "DeviceKey": "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.

AccessToken

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: No

DeviceKey

The key of the device that you want to get information about.

You can get device IDs in the response to a [ListDevices](#) request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-f-]+`

Required: Yes

Response Syntax

```
{
  "Device": {
    "DeviceAttributes": [
      {
        "Name": "string",
        "Value": "string"
      }
    ],
    "DeviceCreateDate": number,
    "DeviceKey": "string",
    "DeviceLastAuthenticatedDate": number,
    "DeviceLastModifiedDate": 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.

Device

Details of the requested device. Includes device information, last-accessed and created dates, and the device key.

Type: [DeviceType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request returns the details of the requested user device.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.GetDevice
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE",
  "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
```

```
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "Device": {
    "DeviceAttributes": [
      {
        "Name": "device_status",
        "Value": "valid"
      },
      {
        "Name": "device_name",
        "Value": "Dart-device"
      },
      {
        "Name": "last_ip_used",
        "Value": "192.0.2.1"
      }
    ],
    "DeviceCreateDate": 1715100742.022,
    "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "DeviceLastAuthenticatedDate": 1715100742.0,
    "DeviceLastModifiedDate": 1723233651.167
  }
}
```

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](#)

GetGroup

Given a user pool ID and a group name, returns information about the user group.

This operation doesn't return group membership. For group membership, see [ListUsersInGroup](#) and [AdminListGroupsForUser](#).

For more information about user pool groups, see [Adding groups to a user pool](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "GroupName": "string",  
  "UserPoolId": "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.

[GroupName](#)

The name of the group that you want to get information about.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool that contains the group that you want to query.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "Group": {
    "CreationDate": number,
    "Description": "string",
    "GroupName": "string",
    "LastModifiedDate": number,
    "Precedence": number,
    "RoleArn": "string",
    "UserPoolId": "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.

Group

A container for the requested group. Includes description, precedence, and IAM role values.

Type: [GroupType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request returns the details of the group testgroup.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.GetGroup
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "GroupName": "testgroup",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
```

```
{
  "Group": {
    "CreationDate": 1681422900.933,
    "Description": "This is a user group for testing",
    "GroupName": "testgroup",
    "LastModifiedDate": 1705447583.756,
    "Precedence": 9,
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/my-SMS-Role",
    "UserPoolId": "us-west-2_EXAMPLE"
  }
}
```

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](#)

GetIdentityProviderByIdentifier

Given the identifier of an identity provider (IdP), for example `examplecorp`, returns information about the user pool configuration for that IdP. For more information about IdPs, see [Third-party IdP sign-in](#).

Request Syntax

```
{
  "IdpIdentifier": "string",
  "UserPoolId": "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.

[IdpIdentifier](#)

The identifier that you assigned to your user pool. The identifier is an alternative name for an IdP that is distinct from the IdP name. For example, an IdP with a name of `MyIdP` might have an identifier of the email domain `example.com`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 40.

Pattern: `[\w\s+=.@- ]+`

Required: Yes

[UserPoolId](#)

The ID of the user pool where you want to get information about the IdP.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w- ]+_[0-9a-zA-Z ]+`

Required: Yes

Response Syntax

```
{
  "IdentityProvider": {
    "AttributeMapping": {
      "string" : "string"
    },
    "CreationDate": number,
    "IdpIdentifiers": [ "string" ],
    "LastModifiedDate": number,
    "ProviderDetails": {
      "string" : "string"
    },
    "ProviderName": "string",
    "ProviderType": "string",
    "UserPoolId": "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.

IdentityProvider

The configuration of the IdP in your user pool. Includes additional identifiers, the IdP name and type, and trust-relationship details like the issuer URL.

Type: [IdentityProviderType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request returns the details of the IdP with the identifier MySSO.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.GetIdentityProviderByIdentifier
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "IdpIdentifier": "MySSO",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "IdentityProvider": {
    "AttributeMapping": {
      "email": "idp_email"
    },
    "CreationDate": 1643741231.169,
    "IdpIdentifiers": [
      "MySSO"
    ],
  },
}
```

```

    "LastModifiedDate": 1703798328.069,
    "ProviderDetails": {
      "ActiveEncryptionCertificate": "[Certificate text]",
      "IDPSignout": "false",
      "MetadataFile": "<md:EntityDescriptor xmlns:md=
\\\"urn:oasis:names:tc:SAML:2.0:metadata\\\" entityID=\\\"http://www.example.com/saml
\\\"><md:IDPSSODescriptor WantAuthnRequestsSigned=\\\"false\\\" protocolSupportEnumeration=
\\\"urn:oasis:names:tc:SAML:2.0:protocol\\\"><md:KeyDescriptor use=
\\\"signing\\\"><ds:KeyInfo xmlns:ds=\\\"http://www.w3.org/2000/09/xmldsig#
\\\"><ds:X509Data><ds:X509Certificate>CERTIFICATE_DATA</ds:X509Certificate></
ds:X509Data></ds:KeyInfo></md:KeyDescriptor><md:SingleLogoutService
  Binding=\\\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST\\\" Location=
\\\"https://example.com/slo/saml\\\"/><md:SingleLogoutService Binding=
\\\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\\\" Location=\\\"https://example.com/
slo/saml\\\"/><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</md:NameIDFormat><md:SingleSignOnService Binding=
\\\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST\\\" Location=\\\"https://example.com/sso/
saml\\\"/><md:SingleSignOnService Binding=\\\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect\\\" Location=\\\"https://example.com/sso/saml\\\"/></md:IDPSSODescriptor></
md:EntityDescriptor>",
      "SLORedirectBindingURI": "https://example.com/slo/saml",
      "SSORedirectBindingURI": "https://example.com/sso/saml"
    },
    "ProviderName": "Corp-SSO",
    "ProviderType": "SAML",
    "UserPoolId": "us-west-2_EXAMPLE"
  }
}

```

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](#)

GetLogDeliveryConfiguration

Given a user pool ID, returns the logging configuration. User pools can export message-delivery error and threat-protection activity logs to external AWS services. For more information, see [Exporting user pool logs](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "UserPoolId": "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.

[UserPoolId](#)

The ID of the user pool that has the logging configuration that you want to view.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "LogDeliveryConfiguration": {
    "LogConfigurations": [
      {
        "CloudWatchLogsConfiguration": {
          "LogGroupArn": "string"
        },
        "EventSource": "string",
        "FirehoseConfiguration": {
          "StreamArn": "string"
        },
        "LogLevel": "string",
        "S3Configuration": {
          "BucketArn": "string"
        }
      }
    ],
    "UserPoolId": "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.

LogDeliveryConfiguration

The logging configuration of the requested user pool. Includes types of logs configured and their destinations.

Type: [LogDeliveryConfigurationType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request returns the log delivery configuration for message-delivery errors to CloudWatch Logs and user activity to Amazon S3.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.GetLogDeliveryConfiguration
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "LogDeliveryConfiguration": {
    "LogConfigurations": [
      {
```

```
        "CloudWatchLogsConfiguration": {
            "LogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:cognito-exported"
        },
        "EventSource": "userNotification",
        "LogLevel": "ERROR"
    },
    {
        "EventSource": "userAuthEvents",
        "LogLevel": "INFO",
        "S3Configuration": {
            "BucketArn": "arn:aws:s3:::amzn-s3-demo-bucket1"
        }
    }
],
"UserPoolId": "us-west-2_EXAMPLE"
}
```

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](#)

GetSigningCertificate

Given a user pool ID, returns the signing certificate for SAML 2.0 federation.

Issued certificates are valid for 10 years from the date of issue. Amazon Cognito issues and assigns a new signing certificate annually. This renewal process returns a new value in the response to `GetSigningCertificate`, but doesn't invalidate the original certificate.

For more information, see [Signing SAML requests](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "UserPoolId": "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.

[UserPoolId](#)

The ID of the user pool where you want to view the signing certificate.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{  
  "Certificate": "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 x.509 certificate that signs SAML 2.0 authentication requests for your user pool.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

Examples

Example

The following example request returns the SAML signing certificate for the requested user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.GetSigningCertificate
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE"
}
```


Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "Certificate": "[Certificate text]"
}
```

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](#)

GetTokensFromRefreshToken

Given a refresh token, issues new ID, access, and optionally refresh tokens for the user who owns the submitted token. This operation issues a new refresh token and invalidates the original refresh token after an optional grace period when refresh token rotation is enabled. If refresh token rotation is disabled, issues new ID and access tokens only.

For information about enabling refresh token rotation and the retry grace period, see [RefreshTokenRotationType](#).

This data type is a request parameter of [CreateUserPoolClient](#) and [UpdateUserPoolClient](#), and a response parameter of [DescribeUserPoolClient](#).

Request Syntax

```
{
  "ClientId": "string",
  "ClientMetadata": {
    "string" : "string"
  },
  "ClientSecret": "string",
  "DeviceKey": "string",
  "RefreshToken": "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.

[ClientId](#)

The app client that issued the refresh token to the user who wants to request new tokens.

Type: String

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

Pattern: `[\w+]`

Required: Yes

ClientMetadata

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ClientSecret

The client secret of the requested app client, if the client has a secret.

Type: String

Length Constraints: Minimum length of 24. Maximum length of 64.

Pattern: `[\w+]+`

Required: No

DeviceKey

When you enable device remembering, Amazon Cognito issues a device key that you can use for device authentication that bypasses multi-factor authentication (MFA). To implement `GetTokensFromRefreshToken` in a user pool with device remembering, you must capture the device key from the initial authentication request. If your application doesn't provide the key of a registered device, Amazon Cognito issues a new one. You must provide the confirmed device key in this request if device remembering is enabled in your user pool.

For more information about device remembering, see [Working with devices](#).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-f-]+`

Required: No

RefreshToken

A valid refresh token that can authorize the request for new tokens. When refresh token rotation is active in the requested app client, this token is invalidated after the request is complete and after an optional grace period.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: Yes

Response Syntax

```
{
  "AuthenticationResult": {
    "AccessToken": "string",
```

```
"ExpiresIn": number,
"IdToken": "string",
"NewDeviceMetadata": {
  "DeviceGroupKey": "string",
  "DeviceKey": "string"
},
"RefreshToken": "string",
"TokenType": "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.

AuthenticationResult

The object that your application receives after authentication. Contains tokens and information for device authentication.

This data type is a response parameter of authentication operations like [InitiateAuth](#), [AdminInitiateAuth](#), [RespondToAuthChallenge](#), [AdminRespondToAuthChallenge](#), and [GetTokensFromRefreshToken](#). [GetTokensFromRefreshToken](#) doesn't return `NewDeviceMetadata`.

Type: [AuthenticationResultType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

RefreshTokenReuseException

This exception is throw when your application requests token refresh with a refresh token that has been invalidated by refresh-token rotation.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

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](#)

GetUICustomization

Given a user pool ID or app client, returns information about classic hosted UI branding that you applied, if any. Returns user-pool level branding information if no app client branding is applied, or if you don't specify an app client ID. Returns an empty object if you haven't applied hosted UI branding to either the client or the user pool. For more information, see [Hosted UI \(classic\) branding](#).

Request Syntax

```
{  
  "ClientId": "string",  
  "UserPoolId": "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.

[ClientId](#)

The ID of the app client that you want to query for branding settings.

Type: String

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

Pattern: `[\w+]`

Required: No

[UserPoolId](#)

The ID of the user pool that you want to query for branding settings.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "UICustomization": {
    "ClientId": "string",
    "CreationDate": number,
    "CSS": "string",
    "CSSVersion": "string",
    "ImageUrl": "string",
    "LastModifiedDate": number,
    "UserPoolId": "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.

UICustomization

Information about the classic hosted UI custom CSS and logo-image branding that you applied to the user pool or app client.

Type: [UICustomizationType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request is for an app client that doesn't have a specific hosted UI customization and inherits it from the user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.GetUICustomization
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ClientId": "1example23456789",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "UICustomization": {
    "ClientId": "ALL",
    "CSS": ".logo-customizable {\n\tmax-width: 60%;\n\tmax-height: 30%;\n}\n\n.banner-customizable {\n\tpadding: 25px 0px 25px 0px;\n\tbackground-color: lightgray;\n}\n\n.label-customizable {\n\tfont-weight: 400;\n}\n\n.textDescription-customizable {\n\tpadding-top: 10px;\n\tpadding-bottom: 10px;\n\tdisplay: block;\n\tfont-size: 16px;\n}\n\n.idpDescription-customizable {\n\tpadding-top: 10px;\n\tpadding-bottom: 10px;\n\tdisplay: block;\n\tfont-size: 16px;\n}\n\n.legalText-customizable {\n\tcolor: #747474;\n\tfont-size: 11px;\n}\n\n.submitButton-customizable {\n\tfont-size: 11px;\n\tfont-weight: normal;\n\tmargin: 20px -15px 10px -13px;\n\theight:
```

```

40px;\n\twidth: 108%;\n\tcolor: #fff;\n\tbackground-color: #337ab7;\n\ttext-align:
center;\n}\n.submitButton-customizable:hover {\n\tcolor: #fff;\n\tbackground-color:
#286090;\n}\n.errorMessage-customizable {\n\tpadding: 5px;\n\tfont-size: 14px;
\n\twidth: 100%;\n\tbackground: #F5F5F5;\n\tborder: 2px solid #D64958;\n\tcolor:
#D64958;\n}\n.inputField-customizable {\n\twidth: 100%;\n\theight: 34px;\n\tcolor:
#555;\n\tbackground-color: #fff;\n\tborder: 1px solid #ccc;\n\tborder-radius:
0px;\n}\n.inputField-customizable:focus {\n\tborder-color: #66afe9;\n\toutline: 0;
\n}\n.idpButton-customizable {\n\theight: 40px;\n\twidth: 100%;\n\twidth: 100%;\n
\ttext-align: center;\n\tmargin-bottom: 15px;\n\tcolor: #fff;\n\tbackground-color:
#5bc0de;\n\tborder-color: #46b8da;\n}\n.idpButton-customizable:hover {\n\tcolor:
#fff;\n\tbackground-color: #31b0d5;\n}\n.socialButton-customizable {\n\tborder-radius:
2px;\n\theight: 40px;\n\tmargin-bottom: 15px;\n\tpadding: 1px;\n\ttext-align: left;\n
\twidth: 100%;\n}\n.redirect-customizable {\n\ttext-align: center;\n}\n.passwordCheck-
notValid-customizable {\n\tcolor: #DF3312;\n}\n.passwordCheck-valid-customizable {\n
\tcolor: #19BF00;\n}\n.background-customizable {\n\tbackground-color: #fff;\n}\n",
    "CSSUrl": "https://auth.example.com/assets/CSS/custom-css.css",
    "CSSVersion": "20210630174334",
    "ImageUrl": "https://auth.example.com/assets/images/image.jpg",
    "UserPoolId": "us-west-2_EXAMPLE"
  }
}

```

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](#)

GetUser

Gets user attributes and and MFA settings for the currently signed-in user.

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{  
  "AccessToken": "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.

[AccessToken](#)

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_=.]`+

Required: Yes

Response Syntax

```
{
  "MFASOptions": [
    {
      "AttributeName": "string",
      "DeliveryMedium": "string"
    }
  ],
  "PreferredMfaSetting": "string",
  "UserAttributes": [
    {
      "Name": "string",
      "Value": "string"
    }
  ],
  "UserMFASettingList": [ "string" ],
  "Username": "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.

MFASOptions

This response parameter is no longer supported. It provides information only about SMS MFA configurations. It doesn't provide information about time-based one-time password (TOTP) software token MFA configurations. To look up information about either type of MFA configuration, use UserMFASettingList instead.

Type: Array of [MFAOptionType](#) objects

PreferredMfaSetting

The user's preferred MFA. Users can prefer SMS message, email message, or TOTP MFA.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

UserAttributes

An array of name-value pairs representing user attributes.

Custom attributes are prepended with the `custom:` prefix.

Type: Array of [AttributeType](#) objects

UserMFASettingList

The MFA options that are activated for the user. The possible values in this list are `SMS_MFA`, `EMAIL_OTP`, and `SOFTWARE_TOKEN_MFA`.

Type: Array of strings

Length Constraints: Minimum length of 0. Maximum length of 131072.

Username

The name of the user that you requested.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request returns the details of the current user.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.GetUser
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "UserAttributes": [
    {
      "Name": "sub",
      "Value": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
    {
      "Name": "identities",
      "Value": "[{\"userId\":\"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222\",
        \"providerName\":\"SignInWithApple\", \"providerType\":\"SignInWithApple\", \"issuer\":null, \"primary\":false, \"dateCreated\":1701125599632}]"
    },
    {
      "Name": "email_verified",
      "Value": "true"
    },
    {
      "Name": "custom:state",
      "Value": "Maine"
    }
  ],
```

```
{
  {
    "Name": "name",
    "Value": "John Doe"
  },
  {
    "Name": "phone_number_verified",
    "Value": "true"
  },
  {
    "Name": "phone_number",
    "Value": "+12065551212"
  },
  {
    "Name": "preferred_username",
    "Value": "jamesdoe"
  },
  {
    "Name": "locale",
    "Value": "EMEA"
  },
  {
    "Name": "email",
    "Value": "jamesdoe@example.com"
  }
],
"Username": "johndoe"
}
```

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](#)

GetUserAttributeVerificationCode

Given an attribute name, sends a user attribute verification code for the specified attribute name to the currently signed-in user.

The user must return the code to Amazon Cognito in a [VerifyUserAttribute](#) request.

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Request Syntax

```
{
```

```
"AccessToken": "string",  
"AttributeName": "string",  
"ClientMetadata": {  
    "string" : "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.

[AccessToken](#)

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws:cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: Yes

[AttributeName](#)

The name of the attribute that the user wants to verify, for example `email`.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\t\n\r ]+`

Required: Yes

[ClientMetadata](#)

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides

the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

Response Syntax

```
{
  "CodeDeliveryDetails": {
    "AttributeName": "string",
    "DeliveryMedium": "string",
    "Destination": "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.

CodeDeliveryDetails

Information about the delivery destination of the user attribute verification code.

Type: [CodeDeliveryDetailsType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

CodeDeliveryFailureException

This exception is thrown when a verification code fails to deliver successfully.

message

The message sent when a verification code fails to deliver successfully.

HTTP Status Code: 400

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request sends a new confirmation code to the current user.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.GetUserAttributeVerificationCode
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE",
  "AttributeName": "email"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
```

```
"CodeDeliveryDetails": {  
  "AttributeName": "email",  
  "DeliveryMedium": "EMAIL",  
  "Destination": "t***@e***"  
}
```

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](#)

GetUserAuthFactors

Lists the authentication options for the currently signed-in user. Returns the following:

1. The user's multi-factor authentication (MFA) preferences.
2. The user's options for choice-based authentication with the USER_AUTH flow.

The list of options in the response to this query are eligible

[RespondToAuthChallenge:ChallengeName](#) selections for PREFERRED_CHALLENGE and are returned in [InitiateAuth:AvailableChallenges](#) when you don't request a PREFERRED_CHALLENGE. The [InitiateAuth:AuthParameters](#) and [RespondToAuthChallenge:ChallengeResponses](#) are specific to each challenge.

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{  
  "AccessToken": "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.

AccessToken

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws:cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: Yes

Response Syntax

```
{
  "ConfiguredUserAuthFactors": [ "string" ],
  "PreferredMfaSetting": "string",
  "UserMFASettingList": [ "string" ],
  "Username": "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.

ConfiguredUserAuthFactors

The authentication types that are available to the user with `USER_AUTH` sign-in, for example `["PASSWORD", "WEB_AUTHN"]`.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 8 items.

Valid Values: `PASSWORD` | `EMAIL_OTP` | `SMS_OTP` | `WEB_AUTHN`

PreferredMfaSetting

The challenge method that Amazon Cognito returns to the user in response to sign-in requests. Users can prefer SMS message, email message, or TOTP MFA.

Change preferred MFA methods for a user with [SetUserMFAPreference](#) or [AdminSetUserMFAPreference](#).

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

[UserMFASettingList](#)

The MFA options that are activated for the user. The possible values in this list are SMS_MFA, EMAIL_OTP, and SOFTWARE_TOKEN_MFA.

SMS and email message MFA are always available to users when your user pool is configured with [CreateUserPool:SmsConfiguration](#) or [CreateUserPool:EmailConfiguration](#) in DEVELOPER mode, respectively. Whether Amazon Cognito presents an MFA challenge and the format of the challenge are set by the PreferredMfa boolean of [SetUserMFAPreference](#).

Type: Array of strings

Length Constraints: Minimum length of 0. Maximum length of 131072.

[Username](#)

The name of the user who is eligible for the authentication factors in the response.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]`+

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request returns the sign-in factors for the current user. They don't have MFA set up.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.GetUserAuthFactors
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "ConfiguredUserAuthFactors": [
    "PASSWORD",
    "EMAIL_OTP",
    "SMS_OTP",
    "WEB_AUTHN"
  ],
  "Username": "testuser"
}
```

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](#)

GetUserPoolMfaConfig

Given a user pool ID, returns configuration for sign-in with WebAuthn authenticators and for multi-factor authentication (MFA). This operation describes the following:

- The WebAuthn relying party (RP) ID and user-verification settings.
- The required, optional, or disabled state of MFA for all user pool users.
- The message templates for email and SMS MFA.
- The enabled or disabled state of time-based one-time password (TOTP) MFA.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "UserPoolId": "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.

[UserPoolId](#)

The ID of the user pool where you want to query WebAuthn and MFA configuration.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "EmailMfaConfiguration": {
    "Message": "string",
    "Subject": "string"
  },
  "MfaConfiguration": "string",
  "SmsMfaConfiguration": {
    "SmsAuthenticationMessage": "string",
    "SmsConfiguration": {
      "ExternalId": "string",
      "SnsCallerArn": "string",
      "SnsRegion": "string"
    }
  },
  "SoftwareTokenMfaConfiguration": {
    "Enabled": boolean
  },
  "WebAuthnConfiguration": {
    "FactorConfiguration": "string",
    "RelyingPartyId": "string",
    "UserVerification": "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.

EmailMfaConfiguration

Shows configuration for user pool email message MFA and sign-in with one-time passwords (OTPs). Includes the subject and body of the email message template for sign-in and MFA messages. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

Type: [EmailMfaConfigType](#) object

MfaConfiguration

Displays the state of multi-factor authentication (MFA) as on, off, or optional. When ON, all users must set up MFA before they can sign in. When OPTIONAL, your application must make a client-side determination of whether a user wants to register an MFA device. For user pools with adaptive authentication with threat protection, choose OPTIONAL.

When MfaConfiguration is OPTIONAL, managed login doesn't automatically prompt users to set up MFA. Amazon Cognito generates MFA prompts in API responses and in managed login for users who have chosen and configured a preferred MFA factor.

Type: String

Valid Values: OFF | ON | OPTIONAL

SmsMfaConfiguration

Shows user pool configuration for SMS message MFA. Includes the message template and the SMS message sending configuration for Amazon SNS.

Type: [SmsMfaConfigType](#) object

SoftwareTokenMfaConfiguration

Shows user pool configuration for time-based one-time password (TOTP) MFA. Includes TOTP enabled or disabled state.

Type: [SoftwareTokenMfaConfigType](#) object

WebAuthnConfiguration

Shows user pool configuration for sign-in with passkey authenticators such as biometric devices and security keys. Includes relying-party configuration, user-verification requirements, and whether passkeys can satisfy MFA requirements.

Type: [WebAuthnConfigurationType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request returns the MFA and WebAuthn configuration for the requested user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.GetUserPoolMfaConfig
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
```

```
{
  "EmailMfaConfiguration": {
    "Message": "Complete your sign-in: use {####}",
    "Subject": "Your sign-in code"
  },
  "MfaConfiguration": "OPTIONAL",
  "SmsMfaConfiguration": {
    "SmsAuthenticationMessage": "Do not share this code with anyone. Your code is {####}.",
    "SmsConfiguration": {
      "ExternalId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "SnsCallerArn": "arn:aws:iam::123456789012:role/service-role/cognito-SMS-Role",
      "SnsRegion": "us-west-2"
    }
  },
  "SoftwareTokenMfaConfiguration": {
    "Enabled": true
  },
  "WebAuthnConfiguration": {
    "RelyingPartyId": "auth.example.com",
    "UserVerification": "preferred"
  }
}
```

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](#)

GlobalSignOut

Invalidates the identity, access, and refresh tokens that Amazon Cognito issued to a user. Call this operation when your user signs out of your app. This results in the following behavior.

- Amazon Cognito no longer accepts *token-authorized* user operations that you authorize with a signed-out user's access tokens. For more information, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Amazon Cognito returns an `Access Token has been revoked` error when your app attempts to authorize a user pools API request with a revoked access token that contains the scope `aws.cognito.signin.user.admin`.

- Amazon Cognito no longer accepts a signed-out user's ID token in a [GetId](#) request to an identity pool with `ServerSideTokenCheck` enabled for its user pool IdP configuration in [CognitoIdentityProvider](#).
- Amazon Cognito no longer accepts a signed-out user's refresh tokens in refresh requests.

Other requests might be valid until your user's token expires. This operation doesn't clear the [managed login](#) session cookie. To clear the session for a user who signed in with managed login or the classic hosted UI, direct their browser session to the [logout endpoint](#).

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{  
  "AccessToken": "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.

[AccessToken](#)

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws:cognito.signin.user.admin`.

Type: String

Pattern: `[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](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

Examples

Example

The following example request signs out the current user.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.GlobalSignOut
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE"
}
```


Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

InitiateAuth

Declares an authentication flow and initiates sign-in for a user in the Amazon Cognito user directory. Amazon Cognito might respond with an additional challenge or an `AuthenticationResult` that contains the outcome of a successful authentication. You can't sign in a user with a federated IdP with `InitiateAuth`. For more information, see [Authentication](#).

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Request Syntax

```
{  
  "AnalyticsMetadata": {  
    "AnalyticsEndpointId": "string"
```

```
{,
  "AuthFlow": "string",
  "AuthParameters": {
    "string" : "string"
  },
  "ClientId": "string",
  "ClientMetadata": {
    "string" : "string"
  },
  "Session": "string",
  "UserContextData": {
    "EncodedData": "string",
    "IpAddress": "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.

[AnalyticsMetadata](#)

Information that supports analytics outcomes with Amazon Pinpoint, including the user's endpoint ID. The endpoint ID is a destination for Amazon Pinpoint push notifications, for example a device identifier, email address, or phone number.

Type: [AnalyticsMetadataType](#) object

Required: No

[AuthFlow](#)

The authentication flow that you want to initiate. Each AuthFlow has linked AuthParameters that you must submit. The following are some example flows.

Include the required [InitiateAuth:AuthParameters](#) for the flow that you choose.

USER_AUTH

The entry point for [choice-based authentication](#) with passwords, one-time passwords, and WebAuthn authenticators. Request a preferred authentication type or review available authentication types. From the offered authentication types, select one in a challenge

response and then authenticate with that method in an additional challenge response. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

USER_SRP_AUTH

Username-password authentication with the Secure Remote Password (SRP) protocol. For more information, see [Use SRP password verification in custom authentication flow](#).

REFRESH_TOKEN_AUTH and REFRESH_TOKEN

Receive new ID and access tokens when you pass a REFRESH_TOKEN parameter with a valid refresh token as the value. For more information, see [Using the refresh token](#).

CUSTOM_AUTH

Custom authentication with Lambda triggers. For more information, see [Custom authentication challenge Lambda triggers](#).

USER_PASSWORD_AUTH

Client-side username-password authentication with the password sent directly in the request. For more information about client-side and server-side authentication, see [SDK authorization models](#).

ADMIN_USER_PASSWORD_AUTH is a flow type of AdminInitiateAuth and isn't valid for InitiateAuth. ADMIN_NO_SRP_AUTH is a legacy server-side username-password flow and isn't valid for InitiateAuth.

Type: String

Valid Values: USER_SRP_AUTH | REFRESH_TOKEN_AUTH | REFRESH_TOKEN
| CUSTOM_AUTH | ADMIN_NO_SRP_AUTH | USER_PASSWORD_AUTH |
ADMIN_USER_PASSWORD_AUTH | USER_AUTH

Required: Yes

[AuthParameters](#)

The authentication parameters. These are inputs corresponding to the AuthFlow that you're invoking.

The following are some authentication flows and their parameters. Add a SECRET_HASH parameter if your app client has a client secret. Add DEVICE_KEY if you want to bypass multi-factor authentication with a remembered device.

USER_AUTH

- USERNAME (required)
- PREFERRED_CHALLENGE. If you don't provide a value for PREFERRED_CHALLENGE, Amazon Cognito responds with the AvailableChallenges parameter that specifies the available sign-in methods.

USER_SRP_AUTH

- USERNAME (required)
- SRP_A (required)

USER_PASSWORD_AUTH

- USERNAME (required)
- PASSWORD (required)

REFRESH_TOKEN_AUTH/REFRESH_TOKEN

- REFRESH_TOKEN(required)

CUSTOM_AUTH

- USERNAME (required)
- ChallengeName: SRP_A (when doing SRP authentication before custom challenges)
- SRP_A: (An SRP_A value) (when doing SRP authentication before custom challenges)

For more information about SECRET_HASH, see [Computing secret hash values](#). For information about DEVICE_KEY, see [Working with user devices in your user pool](#).

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ClientId

The ID of the app client that your user wants to sign in to.

Type: String

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

Pattern: `[\w+]`

Required: Yes

ClientMetadata

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

The `ClientMetadata` value is passed as input to the functions for only the following triggers:

- Pre signup
- Pre authentication
- User migration

This request also invokes the functions for the following triggers, but doesn't pass `ClientMetadata`:

- Post authentication
- Custom message
- Pre token generation
- Create auth challenge
- Define auth challenge
- Custom email sender
- Custom SMS sender

Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool

configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.

- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

Session

The optional session ID from a `ConfirmSignUp` API request. You can sign in a user directly from the sign-up process with the `USER_AUTH` authentication flow. When you pass the session ID to `InitiateAuth`, Amazon Cognito assumes the SMS or email message one-time verification password from `ConfirmSignUp` as the primary authentication factor. You're not required to submit this code a second time. This option is only valid for users who have confirmed their sign-up and are signing in for the first time within the authentication flow session duration of the session ID.

Type: String

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

Required: No

UserContextData

Contextual data about your user session like the device fingerprint, IP address, or location. Amazon Cognito threat protection evaluates the risk of an authentication event based on the context that your app generates and passes to Amazon Cognito when it makes API requests.

For more information, see [Collecting data for threat protection in applications](#).

Type: [UserContextDataType](#) object

Required: No

Response Syntax

```
{
  "AuthenticationResult": {
    "AccessToken": "string",
    "ExpiresIn": number,
    "IdToken": "string",
    "NewDeviceMetadata": {
      "DeviceGroupKey": "string",
      "DeviceKey": "string"
    },
    "RefreshToken": "string",
    "TokenType": "string"
  },
  "AvailableChallenges": [ "string" ],
  "ChallengeName": "string",
  "ChallengeParameters": {
    "string" : "string"
  },
  "Session": "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.

AuthenticationResult

The result of a successful and complete authentication request. This result is only returned if the user doesn't need to pass another challenge. If they must pass another challenge before they get tokens, Amazon Cognito returns a challenge in ChallengeName, ChallengeParameters, and Session response parameters.

Type: [AuthenticationResultType](#) object

AvailableChallenges

This response parameter lists the available authentication challenges that users can select from in [choice-based authentication](#). For example, they might be able to choose between passkey authentication, a one-time password from an SMS message, and a traditional password.

Type: Array of strings

Valid Values: SMS_MFA | EMAIL_OTP | SOFTWARE_TOKEN_MFA | SELECT_MFA_TYPE | MFA_SETUP | PASSWORD_VERIFIER | CUSTOM_CHALLENGE | SELECT_CHALLENGE | DEVICE_SRP_AUTH | DEVICE_PASSWORD_VERIFIER | ADMIN_NO_SRP_AUTH | NEW_PASSWORD_REQUIRED | SMS_OTP | PASSWORD | WEB_AUTHN | PASSWORD_SRP

ChallengeName

The name of an additional authentication challenge that you must respond to.

Collect the challenge response from the user and submit it in a [RespondToAuthChallenge](#) request. To link this response to the new request, include the Session response parameter in the next request.

Possible challenges include the following:

Note

All of the following challenges require USERNAME and, when the app client has a client secret, SECRET_HASH in the parameters. Include a DEVICE_KEY for device authentication.

- WEB_AUTHN: Respond to the challenge with the results of a successful authentication with a WebAuthn authenticator, or passkey, as CREDENTIAL. Examples of WebAuthn authenticators include biometric devices and security keys.
- PASSWORD: Respond with the user's password as PASSWORD.
- PASSWORD_SRP: Respond with the initial SRP secret as SRP_A.
- SELECT_CHALLENGE: Respond with a challenge selection as ANSWER. It must be one of the challenge types in the AvailableChallenges response parameter. Add the parameters of the selected challenge, for example USERNAME and SMS_OTP.
- SMS_MFA: Respond with the code that your user pool delivered in an SMS message, as SMS_MFA_CODE
- EMAIL_MFA: Respond with the code that your user pool delivered in an email message, as EMAIL_MFA_CODE
- EMAIL_OTP: Respond with the code that your user pool delivered in an email message, as EMAIL_OTP_CODE .

- **SMS_OTP**: Respond with the code that your user pool delivered in an SMS message, as **SMS_OTP_CODE**.
- **PASSWORD_VERIFIER**: Respond with the second stage of SRP secrets as **PASSWORD_CLAIM_SIGNATURE**, **PASSWORD_CLAIM_SECRET_BLOCK**, and **TIMESTAMP**.
- **CUSTOM_CHALLENGE**: This is returned if your custom authentication flow determines that the user should pass another challenge before tokens are issued. The parameters of the challenge are determined by your Lambda function and issued in the **ChallengeParameters** of a challenge response.
- **DEVICE_SRP_AUTH**: Respond with the initial parameters of device SRP authentication. For more information, see [Signing in with a device](#).
- **DEVICE_PASSWORD_VERIFIER**: Respond with **PASSWORD_CLAIM_SIGNATURE**, **PASSWORD_CLAIM_SECRET_BLOCK**, and **TIMESTAMP** after client-side SRP calculations. For more information, see [Signing in with a device](#).
- **NEW_PASSWORD_REQUIRED**: For users who are required to change their passwords after successful first login. Respond to this challenge with **NEW_PASSWORD** and any required attributes that Amazon Cognito returned in the **requiredAttributes** parameter. You can also set values for attributes that aren't required by your user pool and that your app client can write.

Amazon Cognito only returns this challenge for users who have temporary passwords. When you create passwordless users, you must provide values for all required attributes.

 Note

In a **NEW_PASSWORD_REQUIRED** challenge response, you can't modify a required attribute that already has a value. In **AdminRespondToAuthChallenge** or **RespondToAuthChallenge**, set a value for any keys that Amazon Cognito returned in the **requiredAttributes** parameter, then use the **AdminUpdateUserAttributes** or **UpdateUserAttributes** API operation to modify the value of any additional attributes.

- **MFA_SETUP**: For users who are required to setup an MFA factor before they can sign in. The MFA types activated for the user pool will be listed in the challenge parameters **MFAS_CAN_SETUP** value.

To set up time-based one-time password (TOTP) MFA, use the session returned in this challenge from `InitiateAuth` or `AdminInitiateAuth` as an input to `AssociateSoftwareToken`. Then, use the session returned by `VerifySoftwareToken` as an input to `RespondToAuthChallenge` or `AdminRespondToAuthChallenge` with challenge name `MFA_SETUP` to complete sign-in.

To set up SMS or email MFA, collect a `phone_number` or `email` attribute for the user. Then restart the authentication flow with an `InitiateAuth` or `AdminInitiateAuth` request.

Type: String

Valid Values: `SMS_MFA` | `EMAIL_OTP` | `SOFTWARE_TOKEN_MFA` | `SELECT_MFA_TYPE` | `MFA_SETUP` | `PASSWORD_VERIFIER` | `CUSTOM_CHALLENGE` | `SELECT_CHALLENGE` | `DEVICE_SRP_AUTH` | `DEVICE_PASSWORD_VERIFIER` | `ADMIN_NO_SRP_AUTH` | `NEW_PASSWORD_REQUIRED` | `SMS_OTP` | `PASSWORD` | `WEB_AUTHN` | `PASSWORD_SRP`

ChallengeParameters

The required parameters of the `ChallengeName` challenge.

Collect the challenge response from the user and submit it in a [RespondToAuthChallenge](#) request. To link this response to the new request, include the `Session` response parameter in the next request.

All challenges require `USERNAME`. They also require `SECRET_HASH` if your app client has a client secret.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Session

The session identifier that links a challenge response to the initial authentication request. If the user must pass another challenge, Amazon Cognito returns a session ID and challenge parameters.

Include this session ID in a [RespondToAuthChallenge](#) API request.

Type: String

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

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UnsupportedOperationException

Exception that is thrown when you attempt to perform an operation that isn't enabled for the user pool client.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example starts the user `testuser` in the `paskey` authentication flow. The user pool and app client have `password`, `paskey`, and `OTP` options. User verification is set to `preferred` for the user pool, so the user isn't required to have a `paskey` with user-verification support.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-east-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.InitiateAuth
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "AuthFlow": "USER_AUTH",
  "ClientId": "1example23456789",
  "AuthParameters": {
    "USERNAME": "testuser",
    "PREFERRED_CHALLENGE": "WEB_AUTHN"
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "AvailableChallenges": [
    "PASSWORD_SRP",
    "PASSWORD",
```



```

        "EMAIL_OTP",
        "WEB_AUTHN"
    ],
    "ChallengeName": "WEB_AUTHN",
    "ChallengeParameters": {
        "CREDENTIAL_REQUEST_OPTIONS": "{\"challenge\":\"[challenge string]\",\"timeout\":"
        \"180000\",\"rpId\":\"auth.example.com\",\"allowCredentials\": [{\"type\":\"public-key\"
        }, {\"id\":\"[key ID]\",\"transports\": []}, {\"type\":\"public-key\", \"id\":\"[key ID]\",
        \"transports\": [\"internal\"]}], \"userVerification\":\"preferred\"}"
    },
    "Session": "AYABeC1-
y8qooiuysEv0uM4wAqQAHQABAAAdTZXJ2aWNlABBDdb2duaXRvVXNlc1Bvb2xzAAEAB2F3cy1rbXMAS2Fybphd3M6a21z0nV
}

```

Example

The following example requests sign-in for the user `testuser` in a user pool where they're eligible for sign in with email OTP.

Sample Request

```

POST HTTP/1.1
Host: cognito-idp.us-east-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.InitiateAuth
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "AuthFlow": "USER_AUTH",
  "ClientId": "lexample23456789",
  "AuthParameters": {
    "USERNAME": "testuser",
    "PREFERRED_CHALLENGE": "EMAIL_OTP"
  }
}

```

Sample Response

```
HTTP/1.1 200 OK
```

```
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "AvailableChallenges": [
    "PASSWORD_SRP",
    "PASSWORD",
    "EMAIL_OTP",
    "WEB_AUTHN"
  ],
  "ChallengeName": "EMAIL_OTP",
  "ChallengeParameters": {
    "CODE_DELIVERY_DELIVERY_MEDIUM": "EMAIL",
    "CODE_DELIVERY_DESTINATION": "t***@e***"
  },
  "Session": "AYABeC1-
y8qooiuysEv0uM4wAqQAHQABAAAdTZXJ2aWNlABBDdb2duaXRvVXNlc1Bvb2xzAAEAB2F3cy1rbXMAS2Fybjpgd3M6a21zOnV
}
```

Example

The following example signs in the user `mytestuser` with analytics data, client metadata, and user context data for advanced security.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.InitiateAuth
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AuthFlow": "USER_PASSWORD_AUTH",
  "ClientId": "1example23456789",
  "AuthParameters": {
    "USERNAME": "mytestuser",
```

```
    "PASSWORD": "This-is-my-test-99!",
    "SECRET_HASH": "oT5ZkS8ctnrhYeeGsGTv0zPhoc/Jd1c05fueBWFVmp8="
  },
  "AnalyticsMetadata": {
    "AnalyticsEndpointId": "d70b2ba36a8c4dc5a04a0451a31a1e12"
  },
  "UserContextData": {
    "EncodedData": "AmazonCognitoAdvancedSecurityData_object",
    "IpAddress": "192.0.2.1"
  },
  "ClientMetadata": {
    "MyTestKey": "MyTestValue"
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "ChallengeName": "SOFTWARE_TOKEN_MFA",
  "ChallengeParameters": {
    "USER_ID_FOR_SRP": "mytestuser",
    "FRIENDLY_DEVICE_NAME": "mytestauthenticator"
  },
  "Session": "AYABeC1-
y8qooiuysEv0uM4wAqQAHQABAAAdTZXJ2aWNlABBDdb2duaXRvVXNlc1Bvb2xzAAEAB2F3cy1rbXMAS2Fybjphd3M6a21zOnV
}
```

Example

The following example exchanges a refresh token for access and ID tokens.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
```

```
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.InitiateAuth
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AuthFlow": "REFRESH_TOKEN",
  "ClientId": "1example23456789",
  "AuthParameters": {
    "REFRESH_TOKEN": "eyJ123abcEXAMPLE",
    "SECRET_HASH": "7P85/EXAMPLE"
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "AuthenticationResult": {
    "AccessToken": "eyJra456defEXAMPLE",
    "ExpiresIn": 3600,
    "IdToken": "eyJra789ghiEXAMPLE",
    "TokenType": "Bearer"
  },
  "ChallengeParameters": {}
}
```

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](#)

ListDevices

Lists the devices that Amazon Cognito has registered to the currently signed-in user. For more information about device authentication, see [Working with user devices in your user pool](#).

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{
  "AccessToken": "string",
  "Limit": number,
  "PaginationToken": "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.

AccessToken

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: Yes

Limit

The maximum number of devices that you want Amazon Cognito to return in the response.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 60.

Required: No

PaginationToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

Required: No

Response Syntax

```
{
  "Devices": [
    {
      "DeviceAttributes": [
        {
          "Name": "string",
          "Value": "string"
        }
      ],
      "DeviceCreateDate": number,
      "DeviceKey": "string",
      "DeviceLastAuthenticatedDate": number,
      "DeviceLastModifiedDate": number
    }
  ]
}
```

```
    }  
  ],  
  "PaginationToken": "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.

[Devices](#)

An array of devices and their details. Each entry that's returned includes device information, last-accessed and created dates, and the device key.

Type: Array of [DeviceType](#) objects

[PaginationToken](#)

The identifier that Amazon Cognito returned with the previous request to this operation. When you include a pagination token in your request, Amazon Cognito returns the next set of items in the list. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request returns the two devices registered by the current user.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ListDevices
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "Devices": [
    {
      "DeviceAttributes": [
        {
          "Name": "device_status",
          "Value": "valid"
        },
        {
          "Name": "device_name",
          "Value": "Dart-device"
        },
        {
          "Name": "last_ip_used",
```

```
        "Value": "192.0.2.1"
      },
    ],
    "DeviceCreateDate": 1715100742.022,
    "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "DeviceLastAuthenticatedDate": 1715100742.0,
    "DeviceLastModifiedDate": 1723233651.167
  },
  {
    "DeviceAttributes": [
      {
        "Name": "device_status",
        "Value": "valid"
      },
      {
        "Name": "last_ip_used",
        "Value": "192.0.2.2"
      }
    ],
    "DeviceCreateDate": 1726856147.993,
    "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "DeviceLastAuthenticatedDate": 1726856147.0,
    "DeviceLastModifiedDate": 1726856147.993
  }
]
}
```

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](#)

ListGroups

Given a user pool ID, returns user pool groups and their details.

This operation doesn't return group membership. For group membership, see [ListUsersInGroup](#) and [AdminListGroupsForUser](#). For more information about user pool groups, see [Adding groups to a user pool](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "Limit": number,  
  "NextToken": "string",  
  "UserPoolId": "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.

[Limit](#)

The maximum number of groups that you want Amazon Cognito to return in the response.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 60.

Required: No

NextToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\S]+`

Required: No

UserPoolId

The ID of the user pool where you want to list user groups.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "Groups": [
    {
      "CreationDate": number,
      "Description": "string",
      "GroupName": "string",
      "LastModifiedDate": number,
      "Precedence": number,
      "RoleArn": "string",
```

```
    "UserPoolId": "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.

Groups

An array of groups and their details. Each entry that's returned includes description, precedence, and IAM role values.

Type: Array of [GroupType](#) objects

NextToken

The identifier that Amazon Cognito returned with the previous request to this operation. When you include a pagination token in your request, Amazon Cognito returns the next set of items in the list. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\S]+`

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request lists two groups in a user pool that has a Facebook identity provider.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ListGroups
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE",
  "Limit": 2
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "Groups": [
    {
      "CreationDate": 1681760899.633,
      "Description": "My test group",
      "GroupName": "testgroup",
      "LastModifiedDate": 1681760899.633,
      "Precedence": 1,
      "UserPoolId": "us-west-2_EXAMPLE"
    },
    {
```

```
        "CreationDate": 1642632749.051,  
        "Description": "Autogenerated group for users who sign in using Facebook",  
        "GroupName": "us-west-2_EXAMPLE_Facebook",  
        "LastModifiedDate": 1642632749.051,  
        "UserPoolId": "us-west-2_EXAMPLE"  
    }  
],  
"NextToken": "[Pagination token]"  
}
```

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](#)

ListIdentityProviders

Given a user pool ID, returns information about configured identity providers (IdPs). For more information about IdPs, see [Third-party IdP sign-in](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "MaxResults": number,  
  "NextToken": "string",  
  "UserPoolId": "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.

MaxResults

The maximum number of IdPs that you want Amazon Cognito to return in the response.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 60.

Required: No

NextToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

Required: No

UserPoolId

The ID of the user pool where you want to list IdPs.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "NextToken": "string",
  "Providers": [
    {
      "CreationDate": number,
      "LastModifiedDate": number,
      "ProviderName": "string",
      "ProviderType": "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.

NextToken

The identifier that Amazon Cognito returned with the previous request to this operation. When you include a pagination token in your request, Amazon Cognito returns the next set of items in the list. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

Providers

An array of the IdPs in your user pool. For each, the response includes identifiers, the IdP name and type, and trust-relationship details like the issuer URL.

Type: Array of [ProviderDescription](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request returns the two configured IdPs in the requested user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ListIdentityProviders
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "Providers": [
    {
      "CreationDate": 1619477386.504,
      "LastModifiedDate": 1703798328.142,
      "ProviderName": "Azure",
      "ProviderType": "SAML"
    },
    {
      "CreationDate": 1642698776.175,
      "LastModifiedDate": 1642699086.453,
      "ProviderName": "LoginWithAmazon",
      "ProviderType": "LoginWithAmazon"
    }
  ]
}
```


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](#)

ListResourceServers

Given a user pool ID, returns all resource servers and their details. For more information about resource servers, see [Access control with resource servers](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "MaxResults": number,  
  "NextToken": "string",  
  "UserPoolId": "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.

[MaxResults](#)

The maximum number of resource servers that you want Amazon Cognito to return in the response.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 50.

Required: No

NextToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

Required: No

UserPoolId

The ID of the user pool where you want to list resource servers.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "NextToken": "string",
  "ResourceServers": [
    {
      "Identifier": "string",
      "Name": "string",
      "Scopes": [
        {
          "ScopeDescription": "string",
          "ScopeName": "string"
        }
      ]
    }
  ]
}
```

```
    ],  
    "UserPoolId": "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.

NextToken

The identifier that Amazon Cognito returned with the previous request to this operation. When you include a pagination token in your request, Amazon Cognito returns the next set of items in the list. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

ResourceServers

An array of resource servers and the details of their configuration. For each, the response includes names, identifiers, and custom scopes.

Type: Array of [ResourceServerType](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request returns the two configured resource servers in the requested user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ListResourceServers
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "ResourceServers": [
    {
      "Identifier": "myapi.example.com",
      "Name": "Example API with custom access control scopes",
      "Scopes": [
        {
          "ScopeDescription": "International customers",
          "ScopeName": "international.read"
        },
        {
          "ScopeDescription": "Domestic customers",
```

```
        "ScopeName": "domestic.read"
      },
    ],
    "UserPoolId": "us-west-2_EXAMPLE"
  },
  {
    "Identifier": "myapi2.example.com",
    "Name": "Another example API for access control",
    "Scopes": [
      {
        "ScopeDescription": "B2B customers",
        "ScopeName": "b2b.read"
      }
    ],
    "UserPoolId": "us-west-2_EXAMPLE"
  }
]
```

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](#)

ListTagsForResource

Lists the tags that are assigned to an Amazon Cognito user pool. For more information, see [Tagging resources](#).

Request Syntax

```
{  
  "ResourceArn": "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.

[ResourceArn](#)

The Amazon Resource Name (ARN) of the user pool that the tags are assigned to.

Type: String

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

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

Required: Yes

Response Syntax

```
{  
  "Tags": {  
    "string" : "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 tags that are assigned to the user pool.

Type: String to string map

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

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

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request returns the tag keys and values for the requested user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ListTagsForResource
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
Signature=<Signature>
```

```
Content-Length: <PayloadSizeBytes>
{
  "ResourceArn": "arn:aws:cognito-idp:us-west-2:123456789012:userpool/us-
west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "Tags": {
    "administrator": "Jie",
    "tenant": "ExampleCorp"
  }
}
```

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](#)

ListTerms

Returns details about all terms documents for the requested user pool.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "MaxResults": number,  
  "NextToken": "string",  
  "UserPoolId": "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.

[MaxResults](#)

The maximum number of terms documents that you want Amazon Cognito to return in the response.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 60.

Required: No

NextToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

UserPoolId

The ID of the user pool where you want to list terms documents.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "NextToken": "string",
  "Terms": [
    {
      "CreationDate": number,
      "Enforcement": "string",
      "LastModifiedDate": number,
      "TermsId": "string",
      "TermsName": "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.

[NextToken](#)

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

[Terms](#)

A summary of the requested terms documents. Includes unique identifiers for later changes to the terms documents.

Type: Array of [TermsDescriptionType](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example operation lists all terms documents for a user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ListTerms
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "UserPoolId": "us-east-1_EXAMPLE",
  "MaxResults": 10
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "Terms": [
    {
      "CreationDate": 1755795432.101,
      "Enforcement": "NONE",
      "LastModifiedDate": 1755795478.934,
      "TermsId": "b2c3d4e5-6789-01bc-def0-EXAMPLE22222",
      "TermsName": "terms-of-use"
    },
    {
      "CreationDate": 1755796023.445,
      "Enforcement": "NONE",
      "LastModifiedDate": 1755796089.712,
      "TermsId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "TermsName": "privacy-policy"
    }
  ]
}
```



```
}
```

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](#)

ListUserImportJobs

Given a user pool ID, returns user import jobs and their details. Import jobs are retained in user pool configuration so that you can stage, stop, start, review, and delete them. For more information about user import, see [Importing users from a CSV file](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "MaxResults": number,
  "PaginationToken": "string",
  "UserPoolId": "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.

[MaxResults](#)

The maximum number of import jobs that you want Amazon Cognito to return in the response.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 60.

Required: Yes

PaginationToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

Required: No

UserPoolId

The ID of the user pool where you want to list import jobs.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "PaginationToken": "string",
  "UserImportJobs": [
    {
      "CloudWatchLogsRoleArn": "string",
      "CompletionDate": number,
      "CompletionMessage": "string",
      "CreationDate": number,
      "FailedUsers": number,
      "ImportedUsers": number,
      "JobId": "string",
      "JobName": "string",
```

```
    "PreSignedUrl": "string",
    "SkippedUsers": number,
    "StartDate": number,
    "Status": "string",
    "UserPoolId": "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.

PaginationToken

The identifier that Amazon Cognito returned with the previous request to this operation. When you include a pagination token in your request, Amazon Cognito returns the next set of items in the list. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

UserImportJobs

An array of user import jobs from the requested user pool. For each, the response includes logging destination, status, and the Amazon S3 pre-signed URL for CSV upload.

Type: Array of [UserImportJobType](#) 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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request returns the first three import jobs in the requested user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ListUserImportJobs
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE",
  "MaxResults": 3
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "PaginationToken": "us-west-2_EXAMPLE#import-example3#1667948397084",
  "UserImportJobs": [
    {
      "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/
Cognito-UserImport-Role",
      "CompletionDate": 1735329786.142,
      "CompletionMessage": "The user import job has expired.",
      "CreationDate": 1735241621.022,
      "FailedUsers": 0,
```

```

        "ImportedUsers": 0,
        "JobId": "import-example1",
        "JobName": "Test-import-job-1",
        "PreSignedUrl": "https://aws-cognito-idp-user-import-pdx.s3.us-
west-2.amazonaws.com/123456789012/us-west-2_EXAMPLE/import-mAgUtd8PMm?X-Amz-Security-
Token=[token]&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20241226T193341Z&X-
Amz-SignedHeaders=host%3Bx-amz-server-side-encryption&X-Amz-Expires=899&X-Amz-
Credential=[credential]&X-Amz-Signature=[signature]",
        "SkippedUsers": 0,
        "Status": "Expired",
        "UserPoolId": "us-west-2_EXAMPLE"
    },
    {
        "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/
Cognito-UserImport-Role",
        "CompletionDate": 1681509058.408,
        "CompletionMessage": "Too many users have failed or been skipped during the
import.",
        "CreationDate": 1681509001.477,
        "FailedUsers": 1,
        "ImportedUsers": 0,
        "JobId": "import-example2",
        "JobName": "Test-import-job-2",
        "PreSignedUrl": "https://aws-cognito-idp-user-import-pdx.s3.us-
west-2.amazonaws.com/123456789012/us-west-2_EXAMPLE/import-mAgUtd8PMm?X-Amz-Security-
Token=[token]&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20241226T193341Z&X-
Amz-SignedHeaders=host%3Bx-amz-server-side-encryption&X-Amz-Expires=899&X-Amz-
Credential=[credential]&X-Amz-Signature=[signature]",
        "SkippedUsers": 0,
        "StartDate": 1681509057.965,
        "Status": "Failed",
        "UserPoolId": "us-west-2_EXAMPLE"
    },
    {
        "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/
Cognito-UserImport-Role",
        "CompletionDate": 1.667864578676E9,
        "CompletionMessage": "Import Job Completed Successfully.",
        "CreationDate": 1.667864480281E9,
        "FailedUsers": 0,
        "ImportedUsers": 6,
        "JobId": "import-example3",
        "JobName": "Test-import-job-3",

```

```
    "PreSignedUrl": "https://aws-cognito-idp-user-import-pdx.s3.us-west-2.amazonaws.com/123456789012/us-west-2_EXAMPLE/import-mAgUtd8PMm?X-Amz-Security-Token=[token]&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20241226T193341Z&X-Amz-SignedHeaders=host%3Bx-amz-server-side-encryption&X-Amz-Expires=899&X-Amz-Credential=[credential]&X-Amz-Signature=[signature]",
    "SkippedUsers": 0,
    "StartDate": 1.667864578167E9,
    "Status": "Succeeded",
    "UserPoolId": "us-west-2_EXAMPLE"
  }
]
```

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](#)

ListUserPoolClients

Given a user pool ID, lists app clients. App clients are sets of rules for the access that you want a user pool to grant to one application. For more information, see [App clients](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "MaxResults": number,  
  "NextToken": "string",  
  "UserPoolId": "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.

MaxResults

The maximum number of app clients that you want Amazon Cognito to return in the response.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 60.

Required: No

NextToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\S]+`

Required: No

UserPoolId

The ID of the user pool where you want to list user pool clients.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "NextToken": "string",
  "UserPoolClients": [
    {
      "ClientId": "string",
      "ClientName": "string",
      "UserPoolId": "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.

NextToken

The identifier that Amazon Cognito returned with the previous request to this operation. When you include a pagination token in your request, Amazon Cognito returns the next set of items in the list. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\S]+`

UserPoolClients

An array of app clients and their details. Includes app client ID and name.

To get more information about one app client, retrieve an app client ID and add it to a [DescribeUserPoolClient](#) request.

Type: Array of [UserPoolClientDescription](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request returns the first three app clients in the requested user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ListUserPoolClients
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "MaxResults": 3,
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "NextToken": "[Pagination token]",
  "UserPoolClients": [
    {
      "ClientId": "1example23456789",
      "ClientName": "app-client-1",
      "UserPoolId": "us-west-2_EXAMPLE"
    },
    {
      "ClientId": "2example34567890",
      "ClientName": "app-client-2",
      "UserPoolId": "us-west-2_EXAMPLE"
    },
    {
      "ClientId": "3example45678901",
      "ClientName": "app-client-3",
      "UserPoolId": "us-west-2_EXAMPLE"
    }
  ]
}
```

```
}
```

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](#)

ListUserPoolClientSecrets

Lists all client secrets associated with a user pool app client. Returns metadata about the secrets. The response does not include pagination tokens as there are only 2 secrets at any given time and we return both with every ListUserPoolClientSecrets call. For security reasons, the response never reveals the actual secret value in ClientSecretValue.

Request Syntax

```
{  
  "ClientId": "string",  
  "UserPoolId": "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.

ClientId

The ID of the app client whose secrets you want to list.

Type: String

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

Pattern: `[\w+]`

Required: Yes

UserPoolId

The ID of the user pool that contains the app client.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "ClientSecrets": [
    {
      "ClientSecretCreateDate": number,
      "ClientSecretId": "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.

[ClientSecrets](#)

A list of client secret descriptors containing the identifier and creation date for each secret. For security reasons, the response never reveals the actual secret value in ClientSecretValue.

Type: Array of [ClientSecretListDescriptorType](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalServerErrorException

This exception is thrown when Amazon Cognito encounters an internal server error.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

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](#)

ListUserPools

Lists user pools and their details in the current AWS account.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "MaxResults": number,  
  "NextToken": "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.

MaxResults

The maximum number of user pools that you want Amazon Cognito to return in the response.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 60.

Required: Yes

NextToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

Required: No

Response Syntax

```
{
  "NextToken": "string",
  "UserPools": [
    {
      "CreationDate": number,
      "Id": "string",
      "LambdaConfig": {
        "CreateAuthChallenge": "string",
        "CustomEmailSender": {
          "LambdaArn": "string",
          "LambdaVersion": "string"
        },
        "CustomMessage": "string",
        "CustomSMSSEnder": {
          "LambdaArn": "string",
          "LambdaVersion": "string"
        },
        "DefineAuthChallenge": "string",
        "InboundFederation": {
          "LambdaArn": "string",
          "LambdaVersion": "string"
        },
        "KMSKeyID": "string",
```

```
    "PostAuthentication": "string",
    "PostConfirmation": "string",
    "PreAuthentication": "string",
    "PreSignUp": "string",
    "PreTokenGeneration": "string",
    "PreTokenGenerationConfig": {
        "LambdaArn": "string",
        "LambdaVersion": "string"
    },
    "UserMigration": "string",
    "VerifyAuthChallengeResponse": "string"
},
"LastModifiedDate": number,
"Name": "string",
"Status": "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.

NextToken

The identifier that Amazon Cognito returned with the previous request to this operation. When you include a pagination token in your request, Amazon Cognito returns the next set of items in the list. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

UserPools

An array of user pools and their configuration details.

Type: Array of [UserPoolDescriptionType](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request lists the first three user pools in the AWS account associated with the user that signed the request.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ListUserPools
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "MaxResults": 3
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "NextToken": "[Pagination token]",
  "UserPools": [
    {
      "CreationDate": 1681502497.741,
      "Id": "us-west-2_EXAMPLE1",
      "LambdaConfig": {
        "CustomMessage": "arn:aws:lambda:us-
east-1:123456789012:function:MyFunction",
```

```
        "PreSignUp": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
        "PreTokenGeneration": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
        "PreTokenGenerationConfig": {
            "LambdaArn": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction",
            "LambdaVersion": "V1_0"
        },
        "LastModifiedDate": 1681502497.741,
        "Name": "user pool 1"
    },
    {
        "CreationDate": 1686064178.717,
        "Id": "us-west-2_EXAMPLE2",
        "LambdaConfig": {
        },
        "LastModifiedDate": 1686064178.873,
        "Name": "user pool 2"
    },
    {
        "CreationDate": 1627681712.237,
        "Id": "us-west-2_EXAMPLE3",
        "LambdaConfig": {
            "UserMigration": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction"
        },
        "LastModifiedDate": 1678486942.479,
        "Name": "user pool 3"
    }
]
}
```

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](#)

ListUsers

Given a user pool ID, returns a list of users and their basic details in a user pool.

This operation is eventually consistent. You might experience a delay before results are up-to-date. To validate the existence or configuration of an individual user, use `AdminGetUser`.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "AttributesToGet": [ "string" ],  
  "Filter": "string",  
  "Limit": number,  
  "PaginationToken": "string",  
  "UserPoolId": "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.

AttributesToGet

A JSON array of user attribute names, for example `given_name`, that you want Amazon Cognito to include in the response for each user. When you don't provide an `AttributesToGet` parameter, Amazon Cognito returns all attributes for each user.

Use `AttributesToGet` with required attributes in your user pool, or in conjunction with `Filter`. Amazon Cognito returns an error if not all users in the results have set a value for the attribute you request. Attributes that you can't filter on, including custom attributes, must have a value set in every user profile before an `AttributesToGet` parameter returns results.

Type: Array of strings

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\t\n\r ]+`

Required: No

Filter

A filter string of the form `"AttributeName Filter-Type "AttributeValue"`. Quotation marks within the filter string must be escaped using the backslash (`\`) character. For example, `"family_name = \"Reddy\""`.

- *AttributeName*: The name of the attribute to search for. You can only search for one attribute at a time.
- *Filter-Type*: For an exact match, use `=`, for example, `"given_name = \"Jon\""`. For a prefix ("starts with") match, use `^=`, for example, `"given_name ^= \"Jon\""`.
- *AttributeValue*: The attribute value that must be matched for each user.

If the filter string is empty, `ListUsers` returns all users in the user pool.

You can only search for the following standard attributes:

- `username` (case-sensitive)
- `email`
- `phone_number`
- `name`
- `given_name`
- `family_name`
- `preferred_username`
- `cognito:user_status` (called **Status** in the Console) (case-insensitive)
- `status` (called **Enabled** in the Console) (case-sensitive)
- `sub`

Custom attributes aren't searchable.

 Note

You can also list users with a client-side filter. The server-side filter matches no more than one attribute. For an advanced search, use a client-side filter with the `--query` parameter of the `list-users` action in the AWS CLI. When you use a client-side filter, `ListUsers` returns a paginated list of zero or more users. You can receive multiple pages in a row with zero results. Repeat the query with each pagination token that is returned until you receive a null pagination token value, and then review the combined result. For more information about server-side and client-side filtering, see [FilteringAWS CLI output](#) in the [AWS Command Line Interface User Guide](#).

For more information, see [Searching for Users Using the ListUsers API](#) and [Examples of Using the ListUsers API](#) in the *Amazon Cognito Developer Guide*.

Type: String

Length Constraints: Maximum length of 256.

Required: No

Limit

The maximum number of users that you want Amazon Cognito to return in the response. In some SDK contexts, this operation might return fewer items than you specify in the `Limit` parameter without having reached the end of the full list. If the response contains a `PaginationToken`, then there are more results.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 60.

Required: No

PaginationToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list.

Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

Required: No

UserPoolId

The ID of the user pool where you want to display or search for users.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "PaginationToken": "string",
  "Users": [
    {
      "Attributes": [
        {
          "Name": "string",
          "Value": "string"
        }
      ],
      "Enabled": boolean,
      "MFAOptions": [
        {
          "AttributeName": "string",
          "DeliveryMedium": "string"
        }
      ],
      "UserCreateDate": number,
      "UserLastModifiedDate": number,
```

```
    "Username": "string",  
    "UserStatus": "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.

PaginationToken

The identifier that Amazon Cognito returned with the previous request to this operation. When you include a pagination token in your request, Amazon Cognito returns the next set of items in the list. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\S]+`

Users

An array of user pool users who match your query, and their attributes. Between different requests, you might observe variations in the sequence that users in this response object are sorted into. The sort order of users isn't guaranteed to follow a single pattern, but the paginated list from a single chain of requests won't return duplicates.

Note

Amazon Cognito creates a profile in your user pool for each local user in your user pool and for each unique user ID from your third-party identity providers (IdPs). When you link users with the [AdminLinkProviderForUser](#) API operation, the output of `ListUsers` displays both the IdP user and the local user that you linked. You can identify IdP users in the `Users` object of this API response by the IdP prefix that Amazon Cognito appends to `Username`.

Type: Array of [UserType](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

This request submits a value for all possible parameters for ListUsers. By iterating the PaginationToken, you can page through and collect all users in a user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-east-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ListUsers
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "AttributesToGet": [
    "email",
    "sub"
  ],
  "Filter": "\"email\"^=\"testuser\"",
  "Limit": 3,
  "PaginationToken": "abcd1234EXAMPLE",
  "UserPoolId": "us-east-1_EXAMPLE"
}
```


Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "PaginationToken": "efgh5678EXAMPLE",
  "Users": [
    {
      "Attributes": [
        {
          "Name": "sub",
          "Value": "eaad0219-2117-439f-8d46-4db20e59268f"
        },
        {
          "Name": "email",
          "Value": "testuser@example.com"
        }
      ],
      "Enabled": true,
      "UserCreateDate": 1682955829.578,
      "UserLastModifiedDate": 1689030181.63,
      "UserStatus": "CONFIRMED",
      "Username": "testuser"
    },
    {
      "Attributes": [
        {
          "Name": "sub",
          "Value": "3b994cfd-0b07-4581-be46-3c82f9a70c90"
        },
        {
          "Name": "email",
          "Value": "testuser2@example.com"
        }
      ],
      "Enabled": true,
      "UserCreateDate": 1684427979.201,
      "UserLastModifiedDate": 1684427979.201,
      "UserStatus": "UNCONFIRMED",
```

```
        "Username": "testuser2"
      },
      {
        "Attributes": [
          {
            "Name": "sub",
            "Value": "5929e0d1-4c34-42d1-9b79-a5ecacfe66f7"
          },
          {
            "Name": "email",
            "Value": "testuser3@example.com"
          }
        ],
        "Enabled": true,
        "UserCreateDate": 1684427823.641,
        "UserLastModifiedDate": 1684427823.641,
        "UserStatus": "UNCONFIRMED",
        "Username": "testuser3@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](#)

ListUsersInGroup

Given a user pool ID and a group name, returns a list of users in the group. For more information about user pool groups, see [Adding groups to a user pool](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "GroupName": "string",  
  "Limit": number,  
  "NextToken": "string",  
  "UserPoolId": "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.

[GroupName](#)

The name of the group that you want to query for user membership.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}] +`

Required: Yes

Limit

The maximum number of groups that you want Amazon Cognito to return in the response. In some SDK contexts, this operation might return fewer items than you specify in the `Limit` parameter without having reached the end of the full list. If the response contains a `PaginationToken`, then there are more results.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 60.

Required: No

NextToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\S] +`

Required: No

UserPoolId

The ID of the user pool where you want to view the membership of the requested group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-] +_[0-9a-zA-Z] +`

Required: Yes

Response Syntax

```
{
  "NextToken": "string",
  "Users": [
    {
      "Attributes": [
        {
          "Name": "string",
          "Value": "string"
        }
      ],
      "Enabled": boolean,
      "MFAOptions": [
        {
          "AttributeName": "string",
          "DeliveryMedium": "string"
        }
      ],
      "UserCreateDate": number,
      "UserLastModifiedDate": number,
      "Username": "string",
      "UserStatus": "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.

NextToken

The identifier that Amazon Cognito returned with the previous request to this operation. When you include a pagination token in your request, Amazon Cognito returns the next set of items in the list. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\S]+`

Users

An array of users who are members in the group, and their attributes.

Type: Array of [UserType](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request lists the two users of the requested group.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ListUsersInGroup
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "GroupName": "testgroup",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "Users": [
    {
      "Attributes": [
        {
          "Name": "sub",
          "Value": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        },
        {
          "Name": "identities",
          "Value": "[{\"userId\":\"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222\",
\"providerName\":\"SignInWithApple\", \"providerType\":\"SignInWithApple\", \"issuer
\":null, \"primary\":false, \"dateCreated\":\"1701125599632}]"
        },
        {
          "Name": "email_verified",
          "Value": "true"
        },
        {
          "Name": "custom:state",
          "Value": "Maine"
        },
        {
          "Name": "name",
          "Value": "John Doe"
        },
        {
          "Name": "phone_number_verified",
          "Value": "true"
        },
        {
          "Name": "phone_number",
          "Value": "+12065551212"
        },
        {
          "Name": "preferred_username",
```



```
        "Value": "jamesdoe"
      },
      {
        "Name": "locale",
        "Value": "EMEA"
      },
      {
        "Name": "email",
        "Value": "jamesdoe@example.com"
      }
    ],
    "Enabled": true,
    "UserCreateDate": 1682955829.578,
    "UserLastModifiedDate": 1736292876.446,
    "Username": "johndoe",
    "UserStatus": "CONFIRMED"
  },
  {
    "Attributes": [
      {
        "Name": "sub",
        "Value": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333"
      },
      {
        "Name": "website",
        "Value": "https://example.com"
      },
      {
        "Name": "email_verified",
        "Value": "true"
      },
      {
        "Name": "custom:state",
        "Value": "New York"
      },
      {
        "Name": "phone_number_verified",
        "Value": "true"
      },
      {
        "Name": "given_name",
        "Value": "Carlos"
      }
    ]
  }
}
```

```
        "Name": "name",
        "Value": "Carlos Salazar"
    },
    {
        "Name": "phone_number",
        "Value": "+12065551212"
    },
    {
        "Name": "family_name",
        "Value": "Salazar"
    },
    {
        "Name": "email",
        "Value": "carlos.salazar@example.com"
    }
],
"Enabled": true,
"UserCreateDate": 1701124862.116,
"UserLastModifiedDate": 1726695472.107,
"Username": "salazarc",
"UserStatus": "CONFIRMED"
}
]
```

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](#)

ListWebAuthnCredentials

Generates a list of the currently signed-in user's registered passkey, or WebAuthn, credentials.

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{  
  "AccessToken": "string",  
  "MaxResults": number,  
  "NextToken": "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.

AccessToken

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: Yes

MaxResults

The maximum number of the user's passkey credentials that you want to return.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 20.

Required: No

NextToken

This API operation returns a limited number of results. The pagination token is an identifier that you can present in an additional API request with the same parameters. When you include the pagination token, Amazon Cognito returns the next set of items after the current list. Subsequent requests return a new pagination token. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\S]+`

Required: No

Response Syntax

```
{
  "Credentials": [
    {
      "AuthenticatorAttachment": "string",
      "AuthenticatorTransports": [ "string" ],
      "CreatedAt": number,
      "CredentialId": "string",
      "FriendlyCredentialName": "string",
      "RelyingPartyId": "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.

Credentials

A list of registered passkeys for a user.

Type: Array of [WebAuthnCredentialDescription](#) objects

NextToken

The identifier that Amazon Cognito returned with the previous request to this operation. When you include a pagination token in your request, Amazon Cognito returns the next set of items in the list. By use of this token, you can paginate through the full list of items.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\S]+`

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request returns details about the one registered passkey for the current user.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ListWebAuthnCredentials
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE"
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
```



```
Connection: keep-alive
{
  "Credentials": [
    {
      "AuthenticatorAttachment": "cross-platform",
      "CreatedAt": 1736293876.115,
      "CredentialId": "8LApgk4-1NUFHbhm2w6Und7-uxcc8coJGsPxiogvHoItc64xWQc3r4CEXAMPLE",
      "FriendlyCredentialName": "Roaming passkey",
      "RelyingPartyId": "auth.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](#)

ResendConfirmationCode

Resends the code that confirms a new account for a user who has signed up in your user pool. Amazon Cognito sends confirmation codes to the user attribute in the `AutoVerifiedAttributes` property of your user pool. When you prompt new users for the confirmation code, include a "Resend code" option that generates a call to this API operation.

When users submit their new confirmation code, send it to your user pool in a [ConfirmSignUp](#) request for account confirmation.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Request Syntax

```
{
```

```
"AnalyticsMetadata": {
  "AnalyticsEndpointId": "string"
},
"ClientId": "string",
"ClientMetadata": {
  "string" : "string"
},
"SecretHash": "string",
"UserContextData": {
  "EncodedData": "string",
  "IpAddress": "string"
},
"Username": "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.

[AnalyticsMetadata](#)

Information that supports analytics outcomes with Amazon Pinpoint, including the user's endpoint ID. The endpoint ID is a destination for Amazon Pinpoint push notifications, for example a device identifier, email address, or phone number.

Type: [AnalyticsMetadataType](#) object

Required: No

[ClientId](#)

The ID of the user pool app client where the user signed up.

Type: String

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

Pattern: `[\w+]`

Required: Yes

ClientMetadata

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

SecretHash

A keyed-hash message authentication code (HMAC) calculated using the secret key of a user pool client and username plus the client ID in the message. For more information about SecretHash, see [Computing secret hash values](#).

Type: String

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

Pattern: `[\w+=/]+`

Required: No

UserContextData

Contextual data about your user session like the device fingerprint, IP address, or location. Amazon Cognito threat protection evaluates the risk of an authentication event based on the context that your app generates and passes to Amazon Cognito when it makes API requests.

For more information, see [Collecting data for threat protection in applications](#).

Type: [UserContextDataType](#) object

Required: No

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If username isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

Response Syntax

```
{
```

```
"CodeDeliveryDetails": {  
  "AttributeName": "string",  
  "DeliveryMedium": "string",  
  "Destination": "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.

[CodeDeliveryDetails](#)

Information about the phone number or email address that Amazon Cognito sent the confirmation code to.

Type: [CodeDeliveryDetailsType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

CodeDeliveryFailureException

This exception is thrown when a verification code fails to deliver successfully.

message

The message sent when a verification code fails to deliver successfully.

HTTP Status Code: 400

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request sends a new email confirmation code to the requested user.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.ResendConfirmationCode
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ClientId": "1example23456789",
  "Username": "akua_mansa"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "CodeDeliveryDetails": {
    "AttributeName": "email",
    "DeliveryMedium": "EMAIL",
    "Destination": "a***@e***"
  }
}
```

```
}
```

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](#)

RespondToAuthChallenge

Some API operations in a user pool generate a challenge, like a prompt for an MFA code, for device authentication that bypasses MFA, or for a custom authentication challenge. A `RespondToAuthChallenge` API request provides the answer to that challenge, like a code or a secure remote password (SRP). The parameters of a response to an authentication challenge vary with the type of challenge.

For more information about custom authentication challenges, see [Custom authentication challenge Lambda triggers](#).

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Request Syntax

```
{
  "AnalyticsMetadata": {
    "AnalyticsEndpointId": "string"
  },
  "ChallengeName": "string",
  "ChallengeResponses": {
    "string" : "string"
  },
  "ClientId": "string",
  "ClientMetadata": {
    "string" : "string"
  },
  "Session": "string",
  "UserContextData": {
    "EncodedData": "string",
    "IpAddress": "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.

[AnalyticsMetadata](#)

Information that supports analytics outcomes with Amazon Pinpoint, including the user's endpoint ID. The endpoint ID is a destination for Amazon Pinpoint push notifications, for example a device identifier, email address, or phone number.

Type: [AnalyticsMetadataType](#) object

Required: No

[ChallengeName](#)

The name of the challenge that you are responding to.

Note

You can't respond to an ADMIN_NO_SRP_AUTH challenge with this operation.

Possible challenges include the following:

Note

All of the following challenges require USERNAME and, when the app client has a client secret, SECRET_HASH in the parameters. Include a DEVICE_KEY for device authentication.

- **WEB_AUTHN**: Respond to the challenge with the results of a successful authentication with a WebAuthn authenticator, or passkey, as CREDENTIAL. Examples of WebAuthn authenticators include biometric devices and security keys.
- **PASSWORD**: Respond with the user's password as PASSWORD.
- **PASSWORD_SRP**: Respond with the initial SRP secret as SRP_A.
- **SELECT_CHALLENGE**: Respond with a challenge selection as ANSWER. It must be one of the challenge types in the AvailableChallenges response parameter. Add the parameters of the selected challenge, for example USERNAME and SMS_OTP.
- **SMS_MFA**: Respond with the code that your user pool delivered in an SMS message, as SMS_MFA_CODE
- **EMAIL_MFA**: Respond with the code that your user pool delivered in an email message, as EMAIL_MFA_CODE
- **EMAIL_OTP**: Respond with the code that your user pool delivered in an email message, as EMAIL_OTP_CODE .
- **SMS_OTP**: Respond with the code that your user pool delivered in an SMS message, as SMS_OTP_CODE.
- **PASSWORD_VERIFIER**: Respond with the second stage of SRP secrets as PASSWORD_CLAIM_SIGNATURE, PASSWORD_CLAIM_SECRET_BLOCK, and TIMESTAMP.
- **CUSTOM_CHALLENGE**: This is returned if your custom authentication flow determines that the user should pass another challenge before tokens are issued. The parameters of the challenge

are determined by your Lambda function and issued in the `ChallengeParameters` of a challenge response.

- `DEVICE_SRP_AUTH`: Respond with the initial parameters of device SRP authentication. For more information, see [Signing in with a device](#).
- `DEVICE_PASSWORD_VERIFIER`: Respond with `PASSWORD_CLAIM_SIGNATURE`, `PASSWORD_CLAIM_SECRET_BLOCK`, and `TIMESTAMP` after client-side SRP calculations. For more information, see [Signing in with a device](#).
- `NEW_PASSWORD_REQUIRED`: For users who are required to change their passwords after successful first login. Respond to this challenge with `NEW_PASSWORD` and any required attributes that Amazon Cognito returned in the `requiredAttributes` parameter. You can also set values for attributes that aren't required by your user pool and that your app client can write.

Amazon Cognito only returns this challenge for users who have temporary passwords. When you create passwordless users, you must provide values for all required attributes.

 Note

In a `NEW_PASSWORD_REQUIRED` challenge response, you can't modify a required attribute that already has a value. In `AdminRespondToAuthChallenge` or `RespondToAuthChallenge`, set a value for any keys that Amazon Cognito returned in the `requiredAttributes` parameter, then use the `AdminUpdateUserAttributes` or `UpdateUserAttributes` API operation to modify the value of any additional attributes.

- `MFA_SETUP`: For users who are required to setup an MFA factor before they can sign in. The MFA types activated for the user pool will be listed in the challenge parameters `MFAS_CAN_SETUP` value.

To set up time-based one-time password (TOTP) MFA, use the session returned in this challenge from `InitiateAuth` or `AdminInitiateAuth` as an input to `AssociateSoftwareToken`. Then, use the session returned by `VerifySoftwareToken` as an input to `RespondToAuthChallenge` or `AdminRespondToAuthChallenge` with challenge name `MFA_SETUP` to complete sign-in.

To set up SMS or email MFA, collect a `phone_number` or `email` attribute for the user. Then restart the authentication flow with an `InitiateAuth` or `AdminInitiateAuth` request.

Type: String

Valid Values: SMS_MFA | EMAIL_OTP | SOFTWARE_TOKEN_MFA | SELECT_MFA_TYPE | MFA_SETUP | PASSWORD_VERIFIER | CUSTOM_CHALLENGE | SELECT_CHALLENGE | DEVICE_SRP_AUTH | DEVICE_PASSWORD_VERIFIER | ADMIN_NO_SRP_AUTH | NEW_PASSWORD_REQUIRED | SMS_OTP | PASSWORD | WEB_AUTHN | PASSWORD_SRP

Required: Yes

ChallengeResponses

The responses to the challenge that you received in the previous request. Each challenge has its own required response parameters. The following examples are partial JSON request bodies that highlight challenge-response parameters.

Important

You must provide a SECRET_HASH parameter in all challenge responses to an app client that has a client secret. Include a DEVICE_KEY for device authentication.

SELECT_CHALLENGE

```
"ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses":  
{ "USERNAME": "[username]", "ANSWER": "[Challenge name]"}
```

Available challenges are PASSWORD, PASSWORD_SRP, EMAIL_OTP, SMS_OTP, and WEB_AUTHN.

Complete authentication in the SELECT_CHALLENGE response for PASSWORD, PASSWORD_SRP, and WEB_AUTHN:

- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses":
 { "ANSWER": "WEB_AUTHN", "USERNAME": "[username]", "CREDENTIAL":
 "[AuthenticationResponseJSON]"}

See [AuthenticationResponseJSON](#).

- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses":
 { "ANSWER": "PASSWORD", "USERNAME": "[username]", "PASSWORD":
 "[password]"}

- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses":
 { "ANSWER": "PASSWORD_SRP", "USERNAME": "[username]", "SRP_A":
 "[SRP_A]"}
 }

For SMS_OTP and EMAIL_OTP, respond with the username and answer. Your user pool will send a code for the user to submit in the next challenge response.

- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses":
 { "ANSWER": "SMS_OTP", "USERNAME": "[username]"}
 }
- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses":
 { "ANSWER": "EMAIL_OTP", "USERNAME": "[username]"}
 }

WEB_AUTHN

```
"ChallengeName": "WEB_AUTHN", "ChallengeResponses": { "USERNAME":  
  "[username]", "CREDENTIAL": "[AuthenticationResponseJSON]"}
```

See [AuthenticationResponseJSON](#).

PASSWORD

```
"ChallengeName": "PASSWORD", "ChallengeResponses": { "USERNAME":  
  "[username]", "PASSWORD": "[password]"}
```

PASSWORD_SRP

```
"ChallengeName": "PASSWORD_SRP", "ChallengeResponses": { "USERNAME":  
  "[username]", "SRP_A": "[SRP_A]"}
```

SMS_OTP

```
"ChallengeName": "SMS_OTP", "ChallengeResponses": {"SMS_OTP_CODE":  
  "[code]", "USERNAME": "[username]"}
```

EMAIL_OTP

```
"ChallengeName": "EMAIL_OTP", "ChallengeResponses": {"EMAIL_OTP_CODE":  
  "[code]", "USERNAME": "[username]"}
```

SMS_MFA

```
"ChallengeName": "SMS_MFA", "ChallengeResponses": {"SMS_MFA_CODE":  
  "[code]", "USERNAME": "[username]"}
```

PASSWORD_VERIFIER

This challenge response is part of the SRP flow. Amazon Cognito requires that your application respond to this challenge within a few seconds. When the response time exceeds this period, your user pool returns a `NotAuthorizedException` error.

```
"ChallengeName": "PASSWORD_VERIFIER", "ChallengeResponses":  
{  
  "PASSWORD_CLAIM_SIGNATURE": "[claim_signature]",  
  "PASSWORD_CLAIM_SECRET_BLOCK": "[secret_block]", "TIMESTAMP":  
  [timestamp], "USERNAME": "[username]"}
```

CUSTOM_CHALLENGE

```
"ChallengeName": "CUSTOM_CHALLENGE", "ChallengeResponses":  
{  
  "USERNAME": "[username]", "ANSWER": "[challenge_answer]"}
```

NEW_PASSWORD_REQUIRED

```
"ChallengeName": "NEW_PASSWORD_REQUIRED", "ChallengeResponses":  
{  
  "NEW_PASSWORD": "[new_password]", "USERNAME": "[username]"}
```

To set any required attributes that `InitiateAuth` returned in an `requiredAttributes` parameter, add `"userAttributes.[attribute_name]": "[attribute_value]"`. This parameter can also set values for writable attributes that aren't required by your user pool.

Note

In a `NEW_PASSWORD_REQUIRED` challenge response, you can't modify a required attribute that already has a value. In `AdminRespondToAuthChallenge` or `RespondToAuthChallenge`, set a value for any keys that Amazon Cognito returned in the `requiredAttributes` parameter, then use the `AdminUpdateUserAttributes` or `UpdateUserAttributes` API operation to modify the value of any additional attributes.

SOFTWARE_TOKEN_MFA

```
"ChallengeName": "SOFTWARE_TOKEN_MFA", "ChallengeResponses":  
{  
  "USERNAME": "[username]", "SOFTWARE_TOKEN_MFA_CODE":  
  [authenticator_code]}
```

DEVICE_SRP_AUTH

```
"ChallengeName": "DEVICE_SRP_AUTH", "ChallengeResponses": {"USERNAME": "[username]", "DEVICE_KEY": "[device_key]", "SRP_A": "[srp_a]"}
```

DEVICE_PASSWORD_VERIFIER

```
"ChallengeName": "DEVICE_PASSWORD_VERIFIER", "ChallengeResponses": {"DEVICE_KEY": "[device_key]", "PASSWORD_CLAIM_SIGNATURE": "[claim_signature]", "PASSWORD_CLAIM_SECRET_BLOCK": "[secret_block]", "TIMESTAMP": [timestamp], "USERNAME": "[username]"}
```

MFA_SETUP

```
"ChallengeName": "MFA_SETUP", "ChallengeResponses": {"USERNAME": "[username]"}, "SESSION": "[Session ID from VerifySoftwareToken]"
```

SELECT_MFA_TYPE

```
"ChallengeName": "SELECT_MFA_TYPE", "ChallengeResponses": {"USERNAME": "[username]", "ANSWER": "[SMS_MFA|EMAIL_MFA|SOFTWARE_TOKEN_MFA]"}
```

For more information about SECRET_HASH, see [Computing secret hash values](#). For information about DEVICE_KEY, see [Working with user devices in your user pool](#).

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ClientId

The ID of the app client where the user is signing in.

Type: String

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

Pattern: `[\w+]`

Required: Yes

ClientMetadata

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

Session

The session identifier that maintains the state of authentication requests and challenge responses. If an `AdminInitiateAuth` or `AdminRespondToAuthChallenge` API request

results in a determination that your application must pass another challenge, Amazon Cognito returns a session with other challenge parameters. Send this session identifier, unmodified, to the next `AdminRespondToAuthChallenge` request.

Type: String

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

Required: No

UserContextData

Contextual data about your user session like the device fingerprint, IP address, or location. Amazon Cognito threat protection evaluates the risk of an authentication event based on the context that your app generates and passes to Amazon Cognito when it makes API requests.

For more information, see [Collecting data for threat protection in applications](#).

Type: [UserContextDataType](#) object

Required: No

Response Syntax

```
{
  "AuthenticationResult": {
    "AccessToken": "string",
    "ExpiresIn": number,
    "IdToken": "string",
    "NewDeviceMetadata": {
      "DeviceGroupKey": "string",
      "DeviceKey": "string"
    },
    "RefreshToken": "string",
    "TokenType": "string"
  },
  "ChallengeName": "string",
  "ChallengeParameters": {
    "string" : "string"
  },
  "Session": "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.

AuthenticationResult

The outcome of a successful authentication process. After your application has passed all challenges, Amazon Cognito returns an `AuthenticationResult` with the JSON web tokens (JWTs) that indicate successful sign-in.

Type: [AuthenticationResultType](#) object

ChallengeName

The name of the next challenge that you must respond to.

Possible challenges include the following:

Note

All of the following challenges require `USERNAME` and, when the app client has a client secret, `SECRET_HASH` in the parameters. Include a `DEVICE_KEY` for device authentication.

- `WEB_AUTHN`: Respond to the challenge with the results of a successful authentication with a WebAuthn authenticator, or passkey, as `CREDENTIAL`. Examples of WebAuthn authenticators include biometric devices and security keys.
- `PASSWORD`: Respond with the user's password as `PASSWORD`.
- `PASSWORD_SRP`: Respond with the initial SRP secret as `SRP_A`.
- `SELECT_CHALLENGE`: Respond with a challenge selection as `ANSWER`. It must be one of the challenge types in the `AvailableChallenges` response parameter. Add the parameters of the selected challenge, for example `USERNAME` and `SMS_OTP`.
- `SMS_MFA`: Respond with the code that your user pool delivered in an SMS message, as `SMS_MFA_CODE`
- `EMAIL_MFA`: Respond with the code that your user pool delivered in an email message, as `EMAIL_MFA_CODE`

- **EMAIL_OTP**: Respond with the code that your user pool delivered in an email message, as **EMAIL_OTP_CODE**.
- **SMS_OTP**: Respond with the code that your user pool delivered in an SMS message, as **SMS_OTP_CODE**.
- **PASSWORD_VERIFIER**: Respond with the second stage of SRP secrets as **PASSWORD_CLAIM_SIGNATURE**, **PASSWORD_CLAIM_SECRET_BLOCK**, and **TIMESTAMP**.
- **CUSTOM_CHALLENGE**: This is returned if your custom authentication flow determines that the user should pass another challenge before tokens are issued. The parameters of the challenge are determined by your Lambda function and issued in the **ChallengeParameters** of a challenge response.
- **DEVICE_SRP_AUTH**: Respond with the initial parameters of device SRP authentication. For more information, see [Signing in with a device](#).
- **DEVICE_PASSWORD_VERIFIER**: Respond with **PASSWORD_CLAIM_SIGNATURE**, **PASSWORD_CLAIM_SECRET_BLOCK**, and **TIMESTAMP** after client-side SRP calculations. For more information, see [Signing in with a device](#).
- **NEW_PASSWORD_REQUIRED**: For users who are required to change their passwords after successful first login. Respond to this challenge with **NEW_PASSWORD** and any required attributes that Amazon Cognito returned in the **requiredAttributes** parameter. You can also set values for attributes that aren't required by your user pool and that your app client can write.

Amazon Cognito only returns this challenge for users who have temporary passwords. When you create passwordless users, you must provide values for all required attributes.

 Note

In a **NEW_PASSWORD_REQUIRED** challenge response, you can't modify a required attribute that already has a value. In **AdminRespondToAuthChallenge** or **RespondToAuthChallenge**, set a value for any keys that Amazon Cognito returned in the **requiredAttributes** parameter, then use the **AdminUpdateUserAttributes** or **UpdateUserAttributes** API operation to modify the value of any additional attributes.

- **MFA_SETUP**: For users who are required to setup an MFA factor before they can sign in. The MFA types activated for the user pool will be listed in the challenge parameters **MFAS_CAN_SETUP** value.

To set up time-based one-time password (TOTP) MFA, use the session returned in this challenge from `InitiateAuth` or `AdminInitiateAuth` as an input to `AssociateSoftwareToken`. Then, use the session returned by `VerifySoftwareToken` as an input to `RespondToAuthChallenge` or `AdminRespondToAuthChallenge` with challenge name `MFA_SETUP` to complete sign-in.

To set up SMS or email MFA, collect a `phone_number` or `email` attribute for the user. Then restart the authentication flow with an `InitiateAuth` or `AdminInitiateAuth` request.

Type: String

Valid Values: `SMS_MFA` | `EMAIL_OTP` | `SOFTWARE_TOKEN_MFA` | `SELECT_MFA_TYPE` | `MFA_SETUP` | `PASSWORD_VERIFIER` | `CUSTOM_CHALLENGE` | `SELECT_CHALLENGE` | `DEVICE_SRP_AUTH` | `DEVICE_PASSWORD_VERIFIER` | `ADMIN_NO_SRP_AUTH` | `NEW_PASSWORD_REQUIRED` | `SMS_OTP` | `PASSWORD` | `WEB_AUTHN` | `PASSWORD_SRP`

ChallengeParameters

The parameters that define your response to the next challenge.

Take the values in `ChallengeParameters` and provide values for them in the `ChallengeResponses` of the next [RespondToAuthChallenge](#) request.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Session

The session identifier that maintains the state of authentication requests and challenge responses. If an `InitiateAuth` or `RespondToAuthChallenge` API request results in a determination that your application must pass another challenge, Amazon Cognito returns a session with other challenge parameters. Send this session identifier, unmodified, to the next `RespondToAuthChallenge` request.

Type: String

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

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AliasExistsException

This exception is thrown when a user tries to confirm the account with an email address or phone number that has already been supplied as an alias for a different user profile. This exception indicates that an account with this email address or phone already exists in a user pool that you've configured to use email address or phone number as a sign-in alias.

message

The message that Amazon Cognito sends to the user when the value of an alias attribute is already linked to another user profile.

HTTP Status Code: 400

CodeMismatchException

This exception is thrown if the provided code doesn't match what the server was expecting.

message

The message provided when the code mismatch exception is thrown.

HTTP Status Code: 400

ExpiredCodeException

This exception is thrown if a code has expired.

message

The message returned when the expired code exception is thrown.

HTTP Status Code: 400

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidPasswordException

This exception is thrown when Amazon Cognito encounters an invalid password.

message

The message returned when Amazon Cognito throws an invalid user password exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

MFAMethodNotFoundException

This exception is thrown when Amazon Cognito can't find a multi-factor authentication (MFA) method.

message

The message returned when Amazon Cognito throws an MFA method not found exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordHistoryPolicyViolationException

The message returned when a user's new password matches a previous password and doesn't comply with the password-history policy.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

SoftwareTokenMFANotFoundException

This exception is thrown when the software token time-based one-time password (TOTP) multi-factor authentication (MFA) isn't activated for the user pool.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example completes sign-in for the user `testuser` with an email-message OTP. Because no additional challenges are required, the request returns an `AuthenticationResult` with ID, access, and refresh tokens.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-east-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.RespondToAuthChallenge
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "ChallengeName": "EMAIL_OTP",
  "ClientId": "1example23456789",
  "UserPoolId": "us-west-2_EXAMPLE",
  "ChallengeResponses": {
    "USERNAME" : "testuser",
    "EMAIL_OTP_CODE": "12345678"
  },
  "Session": "AYABeC1-
y8qooiuysEv0uM4wAqQAHQABAAAdTZXJ2aWNlABBDdb2duaXRvVXNlc1Bvb2xzAAEAB2F3cy1rbXMAS2Fybjphd3M6a21zOnV
}
```

Sample Response

```
HTTP/1.1 200 OK
```

```
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
```

```
{
  "AuthenticationResult": {
    "AccessToken": "eyJra456defEXAMPLE",
    "ExpiresIn": 3600,
    "IdToken": "eyJra789ghiEXAMPLE",
    "RefreshToken": "eyJra123abcEXAMPLE",
    "TokenType": "Bearer"
  },
  "ChallengeParameters": {
  }
}
```

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](#)

RevokeToken

Revokes all of the access tokens generated by, and at the same time as, the specified refresh token. After a token is revoked, you can't use the revoked token to access Amazon Cognito user APIs, or to authorize access to your resource server.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{  
  "ClientId": "string",  
  "ClientSecret": "string",  
  "Token": "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.

ClientId

The ID of the app client where the token that you want to revoke was issued.

Type: String

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

Pattern: `[\w+]`

Required: Yes

ClientSecret

The client secret of the requested app client, if the client has a secret.

Type: String

Length Constraints: Minimum length of 24. Maximum length of 64.

Pattern: `[\w+]`+

Required: No

Token

The refresh token that you want to revoke.

Type: String

Pattern: `[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](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnauthorizedException

Exception that is thrown when the request isn't authorized. This can happen due to an invalid access token in the request.

HTTP Status Code: 400

UnsupportedOperationException

Exception that is thrown when you attempt to perform an operation that isn't enabled for the user pool client.

HTTP Status Code: 400

UnsupportedTokenTypeException

Exception that is thrown when an unsupported token is passed to an operation.

HTTP Status Code: 400

Examples

Example

The following example request revokes the current user's refresh token and access tokens.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.RevokeToken
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ClientId": "1example23456789",
  "Token": "eyJj123abcEXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

SetLogDeliveryConfiguration

Sets up or modifies the logging configuration of a user pool. User pools can export user notification logs and, when threat protection is active, user-activity logs. For more information, see [Exporting user pool logs](#).

Request Syntax

```
{
  "LogConfigurations": [
    {
      "CloudWatchLogsConfiguration": {
        "LogGroupArn": "string"
      },
      "EventSource": "string",
      "FirehoseConfiguration": {
        "StreamArn": "string"
      },
      "LogLevel": "string",
      "S3Configuration": {
        "BucketArn": "string"
      }
    }
  ],
  "UserPoolId": "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.

[LogConfigurations](#)

A collection of the logging configurations for a user pool.

Type: Array of [LogConfigurationType](#) objects

Array Members: Minimum number of 0 items. Maximum number of 2 items.

Required: Yes

UserPoolId

The ID of the user pool where you want to configure logging.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "LogDeliveryConfiguration": {
    "LogConfigurations": [
      {
        "CloudWatchLogsConfiguration": {
          "LogGroupArn": "string"
        },
        "EventSource": "string",
        "FirehoseConfiguration": {
          "StreamArn": "string"
        },
        "LogLevel": "string",
        "S3Configuration": {
          "BucketArn": "string"
        }
      }
    ],
    "UserPoolId": "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.

LogDeliveryConfiguration

The logging configuration that you applied to the requested user pool.

Type: [LogDeliveryConfigurationType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

FeatureUnavailableInTierException

This exception is thrown when a feature you attempted to configure isn't available in your current feature plan.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

A `SetLogDeliveryConfiguration` request that exports `userNotification` logs to a log group and `userAuthEvents` logs to an Amazon S3 bucket.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-east-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.SetLogDeliveryConfiguration
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
```



```
Content-Length: <PayloadSizeBytes>
{
  "LogConfigurations": [
    {
      "CloudWatchLogsConfiguration": {
        "LogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-group:cognito-
exported"
      },
      "EventSource": "userNotification",
      "LogLevel": "ERROR"
    },
    {
      "EventSource": "userAuthEvents",
      "LogLevel": "INFO",
      "S3Configuration": {
        "BucketArn": "arn:aws:s3:::amzn-s3-demo-bucket1"
      }
    }
  ],
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "LogDeliveryConfiguration": {
    "LogConfigurations": [
      {
        "CloudWatchLogsConfiguration": {
          "LogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-group:cognito-
exported"
        },
        "EventSource": "userNotification",
        "LogLevel": "ERROR"
      },
      {
        "EventSource": "userAuthEvents",
```

```

        "LogLevel": "INFO",
        "S3Configuration": {
            "BucketArn": "arn:aws:s3:::amzn-s3-demo-bucket1"
        }
    ],
    "UserPoolId": "us-west-2_EXAMPLE"
}

```

Example

A `SetLogDeliveryConfiguration` request that exports `userAuthEvents` events to a Firehose stream and `userNotification` events to a CloudWatch log group.

Sample Request

```

POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.SetLogDeliveryConfiguration
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "LogConfigurations": [
    {
      "EventSource": "userAuthEvents",
      "FirehoseConfiguration": {
        "StreamArn": "arn:aws:firehose:us-west-2:123456789012:deliverystream/
example-user-pool-activity-exported"
      },
      "LogLevel": "INFO"
    }
  ],
  [
    {
      "CloudWatchLogsConfiguration": {
        "LogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-group:example-user-
pool-error-exported"
      },

```

```
        "EventSource": "userNotification",
        "LogLevel": "ERROR"
    }
],
"UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "LogDeliveryConfiguration": {
    "LogConfigurations": [
      {
        "CloudWatchLogsConfiguration": {
          "LogGroupArn": "arn:aws:firehose:us-
west-2:123456789012:deliverystream/example-user-pool-activity-exported"
        },
        "EventSource": "userNotification",
        "LogLevel": "ERROR"
      },
      {
        "EventSource": "userAuthEvents",
        "FirehoseConfiguration": {
          "StreamArn": "arn:aws:logs:us-west-2:123456789012:log-
group:example-user-pool-error-exported"
        },
        "LogLevel": "INFO"
      }
    ],
    "UserPoolId": "us-west-2_EXAMPLE"
  }
}
```

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](#)

SetRiskConfiguration

Configures threat protection for a user pool or app client. Sets configuration for the following.

- Responses to risks with adaptive authentication
- Responses to vulnerable passwords with compromised-credentials detection
- Notifications to users who have had risky activity detected
- IP-address denylist and allowlist

To set the risk configuration for the user pool to defaults, send this request with only the `UserPoolId` parameter. To reset the threat protection settings of an app client to be inherited from the user pool, send `UserPoolId` and `ClientId` parameters only. To change threat protection to audit-only or off, update the value of `UserPoolAddOns` in an `UpdateUserPool` request. To activate this setting, your user pool must be on the [Plus tier](#).

Request Syntax

```
{
  "AccountTakeoverRiskConfiguration": {
    "Actions": {
      "HighAction": {
        "EventAction": "string",
        "Notify": boolean
      },
      "LowAction": {
        "EventAction": "string",
        "Notify": boolean
      },
      "MediumAction": {
        "EventAction": "string",
        "Notify": boolean
      }
    },
    "NotifyConfiguration": {
      "BlockEmail": {
        "HtmlBody": "string",
        "Subject": "string",
        "TextBody": "string"
      },
      "From": "string",
```

```
    "MfaEmail": {
      "HtmlBody": "string",
      "Subject": "string",
      "TextBody": "string"
    },
    "NoActionEmail": {
      "HtmlBody": "string",
      "Subject": "string",
      "TextBody": "string"
    },
    "ReplyTo": "string",
    "SourceArn": "string"
  }
},
"ClientId": "string",
"CompromisedCredentialsRiskConfiguration": {
  "Actions": {
    "EventAction": "string"
  },
  "EventFilter": [ "string" ]
},
"RiskExceptionConfiguration": {
  "BlockedIPRangeList": [ "string" ],
  "SkippedIPRangeList": [ "string" ]
},
"UserPoolId": "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.

AccountTakeoverRiskConfiguration

The settings for automated responses and notification templates for adaptive authentication with threat protection.

Type: [AccountTakeoverRiskConfigurationType](#) object

Required: No

ClientId

The ID of the app client where you want to set a risk configuration. If `ClientId` is null, then the risk configuration is mapped to `UserPoolId`. When the client ID is null, the same risk configuration is applied to all the clients in the userPool.

When you include a `ClientId` parameter, Amazon Cognito maps the configuration to the app client. When you include both `ClientId` and `UserPoolId`, Amazon Cognito maps the configuration to the app client only.

Type: String

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

Pattern: `[\w+]`

Required: No

CompromisedCredentialsRiskConfiguration

The configuration of automated reactions to detected compromised credentials. Includes settings for blocking future sign-in requests and for the types of password-submission events you want to monitor.

Type: [CompromisedCredentialsRiskConfigurationType](#) object

Required: No

RiskExceptionConfiguration

A set of IP-address overrides to threat protection. You can set up IP-address always-block and always-allow lists.

Type: [RiskExceptionConfigurationType](#) object

Required: No

UserPoolId

The ID of the user pool where you want to set a risk configuration. If you include `UserPoolId` in your request, don't include `ClientId`. When the client ID is null, the same risk configuration is applied to all the clients in the userPool. When you include both `ClientId` and `UserPoolId`, Amazon Cognito maps the configuration to the app client only.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "RiskConfiguration": {
    "AccountTakeoverRiskConfiguration": {
      "Actions": {
        "HighAction": {
          "EventAction": "string",
          "Notify": boolean
        },
        "LowAction": {
          "EventAction": "string",
          "Notify": boolean
        },
        "MediumAction": {
          "EventAction": "string",
          "Notify": boolean
        }
      },
      "NotifyConfiguration": {
        "BlockEmail": {
          "HtmlBody": "string",
          "Subject": "string",
          "TextBody": "string"
        },
        "From": "string",
        "MfaEmail": {
          "HtmlBody": "string",
          "Subject": "string",
          "TextBody": "string"
        },
        "NoActionEmail": {
          "HtmlBody": "string",
          "Subject": "string",
          "TextBody": "string"
        },
        "ReplyTo": "string",
```



```
    "SourceArn": "string"
  },
  "ClientId": "string",
  "CompromisedCredentialsRiskConfiguration": {
    "Actions": {
      "EventAction": "string"
    },
    "EventFilter": [ "string" ]
  },
  "LastModifiedDate": number,
  "RiskExceptionConfiguration": {
    "BlockedIPRangeList": [ "string" ],
    "SkippedIPRangeList": [ "string" ]
  },
  "UserPoolId": "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.

RiskConfiguration

The API response that contains the risk configuration that you set and the timestamp of the most recent change.

Type: [RiskConfigurationType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

CodeDeliveryFailureException

This exception is thrown when a verification code fails to deliver successfully.

message

The message sent when a verification code fails to deliver successfully.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserPoolAddOnNotEnabledException

This exception is thrown when user pool add-ons aren't enabled.

HTTP Status Code: 400

Examples

Example

The following example request configures the requested app client with adaptive authentication actions, compromised-credentials behavior, and IP-address exceptions. It also configures user notification templates.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.SetRiskConfiguration
User-Agent: <UserAgentString>
```

```

Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccountTakeoverRiskConfiguration": {
    "Actions": {
      "HighAction": {
        "EventAction": "MFA_REQUIRED",
        "Notify": true
      },
      "LowAction": {
        "EventAction": "NO_ACTION",
        "Notify": true
      },
      "MediumAction": {
        "EventAction": "MFA_IF_CONFIGURED",
        "Notify": true
      }
    },
    "NotifyConfiguration": {
      "BlockEmail": {
        "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML email\ncontext</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We blocked an\nunrecognized sign-in to your account with this information:\n<ul>\n<li>Time: {login-\ntime}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city}, {country}</li>\n</ul>\nIf this sign-in was not by you, you should change your password and notify us by\nclicking on <a href={one-click-link-invalid}>this link</a>\nIf this sign-in was by\nyou, you can follow <a href={one-click-link-valid}>this link</a> to let us know</pre>\n</body>\n</html>",
        "Subject": "Blocked sign-in attempt",
        "TextBody": "We blocked an unrecognized sign-in to your account with\nthis information:\nTime: {login-time}\nDevice: {device-name}\nLocation: {city},\n{country}\nIf this sign-in was not by you, you should change your password and notify\nus by clicking on {one-click-link-invalid}\nIf this sign-in was by you, you can follow\n{one-click-link-valid} to let us know"
      },
      "From": "admin@example.com",
      "MfaEmail": {
        "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML email\ncontext</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We required you to\nuse multi-factor authentication for the following sign-in attempt:\n<ul>\n<li>Time:\n{login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city}, {country}</\nli>\n</ul>\nIf this sign-in was not by you, you should change your password and notify\nus by clicking on <a href={one-click-link-invalid}>this link</a>\nIf this sign-in was

```

```

    by you, you can follow <a href={one-click-link-valid}>this link</a> to let us know</pre>\n</body>\n</html>",
    "Subject": "New sign-in attempt",
    "TextBody": "We required you to use multi-factor authentication for the following sign-in attempt:\nTime: {login-time}\nDevice: {device-name}\nLocation: {city}, {country}\nIf this sign-in was not by you, you should change your password and notify us by clicking on {one-click-link-invalid}\nIf this sign-in was by you, you can follow {one-click-link-valid} to let us know"
  },
  "NoActionEmail": {
    "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML email context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We observed an unrecognized sign-in to your account with this information:\n<ul>\n<li>Time: {login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city}, {country}</li>\n</ul>\nIf this sign-in was not by you, you should change your password and notify us by clicking on <a href={one-click-link-invalid}>this link</a>\nIf this sign-in was by you, you can follow <a href={one-click-link-valid}>this link</a> to let us know</pre>\n</body>\n</html>",
    "Subject": "New sign-in attempt",
    "TextBody": "We observed an unrecognized sign-in to your account with this information:\nTime: {login-time}\nDevice: {device-name}\nLocation: {city}, {country}\nIf this sign-in was not by you, you should change your password and notify us by clicking on {one-click-link-invalid}\nIf this sign-in was by you, you can follow {one-click-link-valid} to let us know"
  },
  "ReplyTo": "Administrator <admin@example.com>",
  "SourceArn": "arn:aws:ses:us-west-2:123456789012:identity/admin@example.com"
}
},
"ClientId": "1example23456789",
"CompromisedCredentialsRiskConfiguration": {
  "Actions": {
    "EventAction": "BLOCK"
  },
  "EventFilter": [
    "PASSWORD_CHANGE",
    "SIGN_UP",
    "SIGN_IN"
  ]
},
"RiskExceptionConfiguration": {
  "BlockedIPRangeList": [
    "192.0.2.1/32",

```

```
        "192.0.2.2/32"
      ],
      "SkippedIPRangeList": [
        "203.0.113.1/32",
        "203.0.113.2/32"
      ]
    },
    "UserPoolId": "us-west-2_EXAMPLE"
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "RiskConfiguration": {
    "AccountTakeoverRiskConfiguration": {
      "Actions": {
        "HighAction": {
          "EventAction": "MFA_REQUIRED",
          "Notify": true
        },
        "LowAction": {
          "EventAction": "NO_ACTION",
          "Notify": true
        },
        "MediumAction": {
          "EventAction": "MFA_IF_CONFIGURED",
          "Notify": true
        }
      },
      "NotifyConfiguration": {
        "BlockEmail": {
          "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML email context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We blocked an unrecognized sign-in to your account with this information:\n<ul>\n<li>Time: {login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city}, {country}</li>\n</ul>\nIf this sign-in was not by you, you should change your password and notify us by clicking on <a href={one-click-link-invalid}>this link</a>\nIf this sign-in was by"
```

```

you, you can follow <a href={one-click-link-valid}>this link</a> to let us know</pre>
\n</body>\n</html>",
    "Subject": "Blocked sign-in attempt",
    "TextBody": "We blocked an unrecognized sign-in to your account
with this information:\nTime: {login-time}\nDevice: {device-name}\nLocation: {city},
{country}\nIf this sign-in was not by you, you should change your password and notify
us by clicking on {one-click-link-invalid}\nIf this sign-in was by you, you can follow
{one-click-link-valid} to let us know"
  },
  "From": "admin@example.com",
  "MfaEmail": {
    "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML email
context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We required you to
use multi-factor authentication for the following sign-in attempt:\n<ul>\n<li>Time:
{login-time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city}, {country}</
li>\n</ul>\nIf this sign-in was not by you, you should change your password and notify
us by clicking on <a href={one-click-link-invalid}>this link</a>\nIf this sign-in was
by you, you can follow <a href={one-click-link-valid}>this link</a> to let us know</
pre>\n</body>\n</html>",
    "Subject": "New sign-in attempt",
    "TextBody": "We required you to use multi-factor authentication for
the following sign-in attempt:\nTime: {login-time}\nDevice: {device-name}\nLocation:
{city}, {country}\nIf this sign-in was not by you, you should change your password and
notify us by clicking on {one-click-link-invalid}\nIf this sign-in was by you, you can
follow {one-click-link-valid} to let us know"
  },
  "NoActionEmail": {
    "HtmlBody": "<!DOCTYPE html>\n<html>\n<head>\n\t<title>HTML email
context</title>\n\t<meta charset=\"utf-8\">\n</head>\n<body>\n<pre>We observed an
unrecognized sign-in to your account with this information:\n<ul>\n<li>Time: {login-
time}</li>\n<li>Device: {device-name}</li>\n<li>Location: {city}, {country}</li>\n</
ul>\nIf this sign-in was not by you, you should change your password and notify us by
clicking on <a href={one-click-link-invalid}>this link</a>\nIf this sign-in was by
you, you can follow <a href={one-click-link-valid}>this link</a> to let us know</pre>
\n</body>\n</html>",
    "Subject": "New sign-in attempt",
    "TextBody": "We observed an unrecognized sign-in to your account
with this information:\nTime: {login-time}\nDevice: {device-name}\nLocation: {city},
{country}\nIf this sign-in was not by you, you should change your password and notify
us by clicking on {one-click-link-invalid}\nIf this sign-in was by you, you can follow
{one-click-link-valid} to let us know"
  },
  "ReplyTo": "admin@example.com",

```

```

        "SourceArn": "arn:aws:ses:us-west-2:123456789012:identity/
admin@example.com"
    },
    "ClientId": "1example23456789",
    "CompromisedCredentialsRiskConfiguration": {
        "Actions": {
            "EventAction": "BLOCK"
        },
        "EventFilter": [
            "PASSWORD_CHANGE",
            "SIGN_UP",
            "SIGN_IN"
        ]
    },
    "RiskExceptionConfiguration": {
        "BlockedIPRangeList": [
            "192.0.2.1/32",
            "192.0.2.2/32"
        ],
        "SkippedIPRangeList": [
            "203.0.113.1/32",
            "203.0.113.2/32"
        ]
    },
    "UserPoolId": "us-west-2_EXAMPLE"
}
}

```

Example

The following example request clears the threat protection settings of the requested app client.

Sample Request

```

POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.SetRiskConfiguration
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
Signature=<Signature>

```



```
Content-Length: <PayloadSizeBytes>
{
  "ClientId": "1example23456789",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

Example

The following example request resets threat protection settings to default for the requested user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.SetRiskConfiguration
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
```

```
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

SetUICustomization

Configures UI branding settings for domains with the hosted UI (classic) branding version. Your user pool must have a domain. Configure a domain with [CreateUserPoolDomain](#).

Set the default configuration for all clients with a `ClientId` of `ALL`. When the `ClientId` value is an app client ID, the settings you pass in this request apply to that app client and override the default `ALL` configuration.

This operation has no effect on managed login pages. To configure branding for domains with the managed login branding version, see [CreateManagedLoginBranding](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{  
  "ClientId": "string",  
  "CSS": "string",  
  "ImageFile": blob,  
  "UserPoolId": "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.

ClientId

The ID of the app client that you want to customize. To apply a default style to all app clients not configured with client-level branding, set this parameter value to ALL.

Type: String

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

Pattern: `[\w+]`

Required: No

CSS

A plaintext CSS file that contains the custom fields that you want to apply to your user pool or app client. To download a template, go to the Amazon Cognito console. Navigate to your user pool *App clients* tab, select *Login pages*, edit *Hosted UI (classic) style*, and select the link to `CSS template.css`.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ImageFile

The image that you want to set as your login in the classic hosted UI, as a Base64-formatted binary object.

Type: Base64-encoded binary data object

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

UserPoolId

The ID of the user pool where you want to apply branding to the classic hosted UI.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "UICustomization": {
    "ClientId": "string",
    "CreationDate": number,
    "CSS": "string",
    "CSSVersion": "string",
    "ImageUrl": "string",
    "LastModifiedDate": number,
    "UserPoolId": "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.

UICustomization

Information about the hosted UI branding that you applied.

Type: [UICustomizationType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request applies CSS customization and a logo image (the Amazon Cognito logo) to the requested app client.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.SetUICustomization
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ClientId": "1example23456789",
  "CSS": ".logo-customizable {\n\tmax-width: 60%;\n\tmax-height: 30%;\n}\n.banner-
customizable {\n\tpadding: 25px 0px 25px 0px;\n\tbackground-color: lightgray;
\n}\n.label-customizable {\n\tfont-weight: 400;\n}\n.textDescription-customizable {\n
\tpadding-top: 10px;\n\tpadding-bottom: 10px;\n\tdisplay: block;\n\tfont-size: 16px;
\n}\n.idpDescription-customizable {\n\tpadding-top: 10px;\n\tpadding-bottom: 10px;\n
\tdisplay: block;\n\tfont-size: 16px;\n}\n.legalText-customizable {\n\tcolor: #747474;
\n\tfont-size: 11px;\n}\n.submitButton-customizable {\n\tfont-size: 11px;\n\tfont-
weight: normal;\n\tmargin: 20px -15px 10px -13px;\n\theight: 40px;\n\twidth: 108%;\n
\tcolor: #fff;\n\tbackground-color: #337ab7;\n\ttext-align: center;\n}\n.submitButton-
customizable:hover {\n\tcolor: #fff;\n\tbackground-color: #286090;\n}\n.errorMessage-
customizable {\n\tpadding: 5px;\n\tfont-size: 14px;\n\twidth: 100%;\n\tbackground:
#F5F5F5;\n\tborder: 2px solid #D64958;\n\tcolor: #D64958;\n}\n.inputField-customizable
{\n\twidth: 100%;\n\theight: 34px;\n\tcolor: #555;\n\tbackground-color: #fff;\n
\tborder: 1px solid #ccc;\n\tborder-radius: 0px;\n}\n.inputField-customizable:focus
{\n\tborder-color: #66afe9;\n\toutline: 0;\n}\n.idpButton-customizable {\n\theight:
40px;\n\twidth: 100%;\n\twidth: 100%;\n\ttext-align: center;\n\tmargin-bottom: 15px;\n
\tcolor: #fff;\n\tbackground-color: #5bc0de;\n\tborder-color: #46b8da;\n}\n.idpButton-
customizable:hover {\n\tcolor: #fff;\n\tbackground-color: #31b0d5;\n}\n.socialButton-
customizable {\n\tborder-radius: 2px;\n\theight: 40px;\n\tmargin-bottom: 15px;\n
\tpadding: 1px;\n\ttext-align: left;\n\twidth: 100%;\n}\n.redirect-customizable
{\n\ttext-align: center;\n}\n.passwordCheck-notValid-customizable {\n\tcolor:
#DF3312;\n}\n.passwordCheck-valid-customizable {\n\tcolor: #19BF00;\n}\n.background-
customizable {\n\tbackground-color: #fff;\n}\n",
```

```

    "ImageFile":
      "iVBORw0KGgoAAAANSUhEUgAAAFAAAAABQCAMAAAC5zwKfAAAAAXNSR0IArs4c6QAAAAARnQU1BAACxjwv8YQUAAAA2UEXUR
      Cmsfvm6f3y9P/////fM0uqAj
      +yNmu6ZpvnZ3eNabuFNYuZneehzhPKzvPTAxwAAA0iMM1kAAAAASdFJ0U//////////
      AOK/vxIAAAAJcEhZcwAADsMAAA7DAcdvqGQAAAKDSURBVfH7ZfpkoMgEISDHKuEw/
      d/2u2BQWMIrG29o+fVsKatdPMAeZxc3Nz8w+ISekzmB++sYIw/I/tjHzrPp02Tx62EbR2PNxFac
      +jVuKxRaV50IzXkUe76N0CoUuwlvnQKei02gNF0ykot0LRBq/
      nboeWRxAISx2EbsHFoRhK6Igk2JJlwScfQjgt06d0aWwITbEDAe/
      iq8N9kqCw2uCbHkH1YkaXEF8EYeL9RDqT4FhC6XMIIEifdcUwCc4leNyhabadWU60lKYJE10ac3NSPhB5r1aXlSgmr/1lww
      F0L6Q5pZiSG0SfZTSTC0Uhx0CH1AdIoCpTTIjtd
      +VpEjUDDytQH/0Fpc661Aisas/4qmyUItD557pSC0SQQz1x27J
      +meyDGc5zZgfhWuXE1lGgmV0MwmWdeGdzhhjqZV14x5vSj7vsC5JDz/C10Vhp56n2NQt1wQIpury1EPbwyaym
      +IhmAQKoaJkH51wg4cMZ1wQ3QG9efKWW0aDhYwnU6jXjCMdRmm21PArI
      +Pb5DYoh93hq0ZCPlxeGJho/DI15C6sQc/L2sTC47UFBKZGHT6k+z1Xg7WebA0Nr0HTcLMfk/
      Y4Rc65D3iG6WdD7YLSlVqk87bVhUwhnClrx11RsVQwLAA818Mn
      +QEs71BhSFU6orsUfKhHp72XMGYXi4q9c64RXRvzkWurRfG2vI2be/VaNcNgpX0Ebv/
      vio7nPMmj5qujKpQgSaPd1UcVqciHFDNZp0cG1c0Pyi+AamCbIL9fitxAGeFN2Dl
      +3vZubm5u/4fH4Bd14HhIPdwZPAAAAAE1FTkSuQmCC",
      "UserPoolId": "us-west-2_EXAMPLE"
  }

```

Sample Response

```

HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "UICustomization": {
    "ClientId": "1example23456789",
    "CSS": ".logo-customizable {\n\tmax-width: 60%;\n\tmax-height: 30%;
\n}\n.banner-customizable {\n\tpadding: 25px 0px 25px 0px;\n\tbackground-color:
  lightgray;\n}\n.label-customizable {\n\tfont-weight: 400;\n}\n.textDescription-
  customizable {\n\tpadding-top: 10px;\n\tpadding-bottom: 10px;\n\tdisplay: block;\n
\tfont-size: 16px;\n}\n.idpDescription-customizable {\n\tpadding-top: 10px;\n\tpadding-
  bottom: 10px;\n\tdisplay: block;\n\tfont-size: 16px;\n}\n.legalText-customizable
  {\n\tcolor: #747474;\n\tfont-size: 11px;\n}\n.submitButton-customizable {\n\tfont-
  size: 11px;\n\tfont-weight: normal;\n\tmargin: 20px -15px 10px -13px;\n\theight:
  40px;\n\twidth: 108%;\n\tcolor: #fff;\n\tbackground-color: #337ab7;\n\ttext-align:
  center;\n}\n.submitButton-customizable:hover {\n\tcolor: #fff;\n\tbackground-color:
  #286090;\n}\n.errorMessage-customizable {\n\tpadding: 5px;\n\tfont-size: 14px;

```



```

\n\twidth: 100%;\n\tbackground: #F5F5F5;\n\tborder: 2px solid #D64958;\n\tcolor:
#D64958;\n}\n\n.inputField-customizable {\n\twidth: 100%;\n\theight: 34px;\n\tcolor:
#555;\n\tbackground-color: #fff;\n\tborder: 1px solid #ccc;\n\tborder-radius:
0px;\n}\n\n.inputField-customizable:focus {\n\tborder-color: #66afe9;\n\toutline: 0;
\n}\n\n.idpButton-customizable {\n\theight: 40px;\n\twidth: 100%;\n\twidth: 100%;\n
\ttext-align: center;\n\tmargin-bottom: 15px;\n\tcolor: #fff;\n\tbackground-color:
#5bc0de;\n\tborder-color: #46b8da;\n}\n\n.idpButton-customizable:hover {\n\tcolor:
#fff;\n\tbackground-color: #31b0d5;\n}\n\n.socialButton-customizable {\n\tborder-radius:
2px;\n\theight: 40px;\n\tmargin-bottom: 15px;\n\tpadding: 1px;\n\ttext-align: left;\n
\twidth: 100%;\n}\n\n.redirect-customizable {\n\ttext-align: center;\n}\n\n.passwordCheck-
notValid-customizable {\n\tcolor: #DF3312;\n}\n\n.passwordCheck-valid-customizable {\n
\tcolor: #19BF00;\n}\n\n.background-customizable {\n\tbackground-color: #fff;\n}\n\n",
    "CSSUrl": "https://auth.example.com/1example23456789/20250109170543/assets/CSS/
custom-css.css",
    "CSSVersion": "20250109170543",
    "ImageUrl": "https://auth.example.com/1example23456789/20250109170543/assets/
images/image.jpg",
    "UserPoolId": "us-west-2_EXAMPLE"
  }
}

```

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](#)

SetUserMFAPreference

Set the user's multi-factor authentication (MFA) method preference, including which MFA factors are activated and if any are preferred. Only one factor can be set as preferred. The preferred MFA factor will be used to authenticate a user if multiple factors are activated. If multiple options are activated and no preference is set, a challenge to choose an MFA option will be returned during sign-in. If an MFA type is activated for a user, the user will be prompted for MFA during all sign-in attempts unless device tracking is turned on and the device has been trusted. If you want MFA to be applied selectively based on the assessed risk level of sign-in attempts, deactivate MFA for users and turn on Adaptive Authentication for the user pool.

This operation doesn't reset an existing TOTP MFA for a user. To register a new TOTP factor for a user, make an [AssociateSoftwareToken](#) request. For more information, see [TOTP software token MFA](#).

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{
  "AccessToken": "string",
  "EmailMfaSettings": {
    "Enabled": boolean,
    "PreferredMfa": boolean
  },
  "SMSMfaSettings": {
    "Enabled": boolean,
    "PreferredMfa": boolean
  },
}
```

```
"SoftwareTokenMfaSettings": {  
  "Enabled": boolean,  
  "PreferredMfa": boolean  
},  
"WebAuthnMfaSettings": {  
  "Enabled": boolean  
}  
}
```

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.

[AccessToken](#)

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_=.]`+

Required: Yes

[EmailMfaSettings](#)

User preferences for email message MFA. Activates or deactivates email MFA and sets it as the preferred MFA method when multiple methods are available. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

Type: [EmailMfaSettingsType](#) object

Required: No

[SMSMfaSettings](#)

User preferences for SMS message MFA. Activates or deactivates SMS MFA and sets it as the preferred MFA method when multiple methods are available.

Type: [SMSMfaSettingsType](#) object

Required: No

[SoftwareTokenMfaSettings](#)

User preferences for time-based one-time password (TOTP) MFA. Activates or deactivates TOTP MFA and sets it as the preferred MFA method when multiple methods are available. Users must register a TOTP authenticator before they set this as their preferred MFA method.

Type: [SoftwareTokenMfaSettingsType](#) object

Required: No

[WebAuthnMfaSettings](#)

User preferences for passkey MFA. Activates or deactivates passkey MFA for the user. When activated, passkey authentication requires user verification, and passkey sign-in is available when MFA is required. To activate this setting, the `FactorConfiguration` of your user pool `WebAuthnConfiguration` must be `MULTI_FACTOR_WITH_USER_VERIFICATION`. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

Type: [WebAuthnMfaSettingsType](#) 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](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request sets TOTP, SMS, and email MFA active, and TOTP MFA as preferred for the current user.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.SetUserMFAPreference
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
```

```
{
  "AccessToken": "eyJra456defEXAMPLE",
  "SMSMfaSettings": {
    "Enabled": true,
    "PreferredMfa": false
  },
  "EmailMfaSettings": {
    "Enabled": true,
    "PreferredMfa": false
  },
  "SoftwareTokenMfaSettings": {
    "Enabled": true,
    "PreferredMfa": true
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

SetUserPoolMfaConfig

Sets user pool multi-factor authentication (MFA) and passkey configuration. For more information about user pool MFA, see [Adding MFA](#). For more information about WebAuthn passkeys see [Authentication flows](#).

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Request Syntax

```
{
  "EmailMfaConfiguration": {
    "Message": "string",
    "Subject": "string"
  },
  "MfaConfiguration": "string",
  "SmsMfaConfiguration": {
    "SmsAuthenticationMessage": "string",
    "SmsConfiguration": {
      "ExternalId": "string",
      "SnsCallerArn": "string",
      "SnsRegion": "string"
    }
  },
  "SoftwareTokenMfaConfiguration": {
```

```
    "Enabled": boolean
  },
  "UserPoolId": "string",
  "WebAuthnConfiguration": {
    "FactorConfiguration": "string",
    "RelyingPartyId": "string",
    "UserVerification": "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.

[EmailMfaConfiguration](#)

Sets configuration for user pool email message MFA and sign-in with one-time passwords (OTPs). Includes the subject and body of the email message template for sign-in and MFA messages. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

Type: [EmailMfaConfigType](#) object

Required: No

[MfaConfiguration](#)

Sets multi-factor authentication (MFA) to be on, off, or optional. When ON, all users must set up MFA before they can sign in. When OPTIONAL, your application must make a client-side determination of whether a user wants to register an MFA device. For user pools with adaptive authentication with threat protection, choose OPTIONAL.

When MfaConfiguration is OPTIONAL, managed login doesn't automatically prompt users to set up MFA. Amazon Cognito generates MFA prompts in API responses and in managed login for users who have chosen and configured a preferred MFA factor.

Type: String

Valid Values: OFF | ON | OPTIONAL

Required: No

SmsMfaConfiguration

Configures user pool SMS messages for MFA. Sets the message template and the SMS message sending configuration for Amazon SNS.

Type: [SmsMfaConfigType](#) object

Required: No

SoftwareTokenMfaConfiguration

Configures a user pool for time-based one-time password (TOTP) MFA. Enables or disables TOTP.

Type: [SoftwareTokenMfaConfigType](#) object

Required: No

UserPoolId

The user pool ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

WebAuthnConfiguration

The configuration of your user pool for passkey, or WebAuthn, authentication and registration. Includes relying-party configuration, user-verification requirements, and whether passkeys can satisfy MFA requirements.

Type: [WebAuthnConfigurationType](#) object

Required: No

Response Syntax

```
{
```

```
{
  "EmailMfaConfiguration": {
    "Message": "string",
    "Subject": "string"
  },
  "MfaConfiguration": "string",
  "SmsMfaConfiguration": {
    "SmsAuthenticationMessage": "string",
    "SmsConfiguration": {
      "ExternalId": "string",
      "SnsCallerArn": "string",
      "SnsRegion": "string"
    }
  },
  "SoftwareTokenMfaConfiguration": {
    "Enabled": boolean
  },
  "WebAuthnConfiguration": {
    "FactorConfiguration": "string",
    "RelyingPartyId": "string",
    "UserVerification": "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.

EmailMfaConfiguration

Shows configuration for user pool email message MFA and sign-in with one-time passwords (OTPs). Includes the subject and body of the email message template for sign-in and MFA messages. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

Type: [EmailMfaConfigType](#) object

MfaConfiguration

Displays multi-factor authentication (MFA) as on, off, or optional. When ON, all users must set up MFA before they can sign in. When OPTIONAL, your application must make a client-side determination of whether a user wants to register an MFA device. For user pools with adaptive authentication with threat protection, choose OPTIONAL.

When `MfaConfiguration` is `OPTIONAL`, managed login doesn't automatically prompt users to set up MFA. Amazon Cognito generates MFA prompts in API responses and in managed login for users who have chosen and configured a preferred MFA factor.

Type: String

Valid Values: OFF | ON | OPTIONAL

SmsMfaConfiguration

Shows user pool SMS message configuration for MFA and sign-in with SMS-message OTPs. Includes the message template and the SMS message sending configuration for Amazon SNS.

Type: [SmsMfaConfigType](#) object

SoftwareTokenMfaConfiguration

Shows user pool configuration for time-based one-time password (TOTP) MFA. Includes TOTP enabled or disabled state.

Type: [SoftwareTokenMfaConfigType](#) object

WebAuthnConfiguration

The configuration of your user pool for passkey, or WebAuthn, sign-in with authenticators such as biometric and security-key devices. Includes relying-party configuration and settings for user-verification requirements.

Type: [WebAuthnConfigurationType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

FeatureUnavailableInTierException

This exception is thrown when a feature you attempted to configure isn't available in your current feature plan.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the

external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request configures optional MFA in the user pool, message configuration and templates, and WebAuthn.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.SetUserPoolMfaConfig
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "EmailMfaConfiguration": {
    "Message": "Your OTP for MFA or sign-in: use {####}",
    "Subject": "OTP test"
  },
  "MfaConfiguration": "OPTIONAL",
  "SmsMfaConfiguration": {
    "SmsAuthenticationMessage": "Your OTP for MFA or sign-in: use {####}.",
    "SmsConfiguration": {
      "ExternalId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "SnsCallerArn": "arn:aws:iam::123456789012:role/service-role/test-SMS-Role",
      "SnsRegion": "us-west-2"
    }
  },
  "SoftwareTokenMfaConfiguration": {
    "Enabled": true
  },
  "UserPoolId": "us-west-2_EXAMPLE",
  "WebAuthnConfiguration": {
    "RelyingPartyId": "auth.example.com",
    "UserVerification": "preferred"
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
```



```
{
  "EmailMfaConfiguration": {
    "Message": "Your OTP for MFA or sign-in: use {####}",
    "Subject": "OTP test"
  },
  "MfaConfiguration": "OPTIONAL",
  "SmsMfaConfiguration": {
    "SmsAuthenticationMessage": "Your OTP for MFA or sign-in: use {####}.",
    "SmsConfiguration": {
      "ExternalId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "SnsCallerArn": "arn:aws:iam::123456789012:role/service-role/test-SMS-Role",
      "SnsRegion": "us-west-2"
    }
  },
  "SoftwareTokenMfaConfiguration": {
    "Enabled": true
  },
  "WebAuthnConfiguration": {
    "RelyingPartyId": "auth.example.com",
    "UserVerification": "preferred"
  }
}
```

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](#)

SetUserSettings

This action is no longer supported. You can use it to configure only SMS MFA. You can't use it to configure time-based one-time password (TOTP) software token or email MFA.

To configure any or all of the MFA methods, use [SetUserMFAPreference](#) instead.

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{
  "AccessToken": "string",
  "MFAOptions": [
    {
      "AttributeName": "string",
      "DeliveryMedium": "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.

AccessToken

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: [A-Za-z0-9-_=.] +

Required: Yes

MFAOptions

You can use this parameter only to set an SMS configuration that uses SMS for delivery.

Type: Array of [MFAOptionType](#) objects

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](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

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](#)

SignUp

Registers a user with an app client and requests a user name, password, and user attributes in the user pool.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

You might receive a `LimitExceeded` exception in response to this request if you have exceeded a rate quota for email or SMS messages, and if your user pool automatically verifies email addresses or phone numbers. When you get this exception in the response, the user is successfully created and is in an `UNCONFIRMED` state.

You can send a new code with the [ResendConfirmationCode](#) request, or confirm the user as an administrator with an [AdminConfirmSignUp](#) request.

Request Syntax

```
{
  "AnalyticsMetadata": {
    "AnalyticsEndpointId": "string"
  },
  "ClientId": "string",
  "ClientMetadata": {
    "string" : "string"
  },
  "Password": "string",
  "SecretHash": "string",
  "UserAttributes": [
    {
      "Name": "string",
      "Value": "string"
    }
  ],
  "UserContextData": {
    "EncodedData": "string",
    "IpAddress": "string"
  },
  "Username": "string",
  "ValidationData": [
    {
      "Name": "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.

[AnalyticsMetadata](#)

Information that supports analytics outcomes with Amazon Pinpoint, including the user's endpoint ID. The endpoint ID is a destination for Amazon Pinpoint push notifications, for example a device identifier, email address, or phone number.

Type: [AnalyticsMetadataType](#) object

Required: No

[ClientId](#)

The ID of the app client where the user wants to sign up.

Type: String

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

Pattern: `[\w+]`

Required: Yes

[ClientMetadata](#)

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.

- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

Password

The user's proposed password. The password must comply with the [password requirements](#) of your user pool.

Users can sign up without a password when your user pool supports passwordless sign-in with email or SMS OTPs. To create a user with no password, omit this parameter or submit a blank value. You can only create a passwordless user when passwordless sign-in is available.

For more information about passwordless options, see [SignInPolicyType](#), a property of [CreateUserPool](#) and [UpdateUserPool](#).

Type: String

Length Constraints: Maximum length of 256.

Pattern: `[\S]+`

Required: No

SecretHash

A keyed-hash message authentication code (HMAC) calculated using the secret key of a user pool client and username plus the client ID in the message. For more information about `SecretHash`, see [Computing secret hash values](#).

Type: String

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

Pattern: `[\w+=/]+`

Required: No

UserAttributes

An array of name-value pairs representing user attributes.

For custom attributes, include a `custom:` prefix in the attribute name, for example `custom:department`.

Type: Array of [AttributeType](#) objects

Required: No

UserContextData

Contextual data about your user session like the device fingerprint, IP address, or location. Amazon Cognito threat protection evaluates the risk of an authentication event based on the context that your app generates and passes to Amazon Cognito when it makes API requests.

For more information, see [Collecting data for threat protection in applications](#).

Type: [UserContextDataType](#) object

Required: No

Username

The username of the user that you want to sign up. The value of this parameter is typically a username, but can be any alias attribute in your user pool.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]`+

Required: Yes

ValidationData

Temporary user attributes that contribute to the outcomes of your pre sign-up Lambda trigger. This set of key-value pairs are for custom validation of information that you collect from your users but don't need to retain.

Your Lambda function can analyze this additional data and act on it. Your function can automatically confirm and verify select users or perform external API operations like logging user attributes and validation data to Amazon CloudWatch Logs.

For more information about the pre sign-up Lambda trigger, see [Pre sign-up Lambda trigger](#).

Type: Array of [AttributeType](#) objects

Required: No

Response Syntax

```
{
  "CodeDeliveryDetails": {
    "AttributeName": "string",
    "DeliveryMedium": "string",
    "Destination": "string"
  },
  "Session": "string",
  "UserConfirmed": boolean,
  "UserSub": "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.

[CodeDeliveryDetails](#)

In user pools that automatically verify and confirm new users, Amazon Cognito sends users a message with a code or link that confirms ownership of the phone number or email address that they entered. The `CodeDeliveryDetails` object is information about the delivery destination for that link or code.

Collect this code from the user and submit it in a [ConfirmSignUp](#) request.

Type: [CodeDeliveryDetailsType](#) object

[Session](#)

A session Id that you can pass to `ConfirmSignUp` when you want to immediately sign in your user with the `USER_AUTH` flow after they complete sign-up.

Type: String

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

UserConfirmed

Indicates whether the user was automatically confirmed. You can auto-confirm users with a [pre sign-up Lambda trigger](#).

Type: Boolean

UserSub

The unique identifier of the new user, for example a1b2c3d4-5678-90ab-cdef-EXAMPLE11111.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

CodeDeliveryFailureException

This exception is thrown when a verification code fails to deliver successfully.

message

The message sent when a verification code fails to deliver successfully.

HTTP Status Code: 400

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidPasswordException

This exception is thrown when Amazon Cognito encounters an invalid password.

message

The message returned when Amazon Cognito throws an invalid user password exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UsernameExistsException

This exception is thrown when Amazon Cognito encounters a user name that already exists in the user pool.

message

The message returned when Amazon Cognito throws a user name exists exception.

HTTP Status Code: 400

Examples

Example

A sign-up request for the user `mary_major`.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-east-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.SignUp
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "ClientId": "1example23456789",
  "Username": "mary_major",
  "Password": "<Password>",
  "SecretHash": "<Secret hash>",
  "UserAttributes": [
    {
      "Name": "name",
      "Value": "Mary"
    },
    {
      "Name": "email",
      "Value": "mary_major@example.com"
    }
  ]
}
```

```
    },
    {
      "Name": "phone_number",
      "Value": "+12065551212"
    }
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "CodeDeliveryDetails": {
    "AttributeName": "email",
    "DeliveryMedium": "EMAIL",
    "Destination": "m***@e***"
  },
  "UserConfirmed": false,
  "UserSub": "44284a5f-66af-4888-b582-fccc213c51fd"
}
```

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](#)

StartUserImportJob

Instructs your user pool to start importing users from a CSV file that contains their usernames and attributes. For more information about importing users from a CSV file, see [Importing users from a CSV file](#).

To create a job that you can start with this request, see [CreateUserImportJob](#). To generate a template for your import, see [GetCSVHeader](#).

Request Syntax

```
{  
  "JobId": "string",  
  "UserPoolId": "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.

[JobId](#)

The ID of a user import job that you previously created.

To get information about jobs that you can start, see [ListUserImportJobs](#).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: import-[0-9a-zA-Z-]+

Required: Yes

[UserPoolId](#)

The ID of the user pool that you want to start importing users into.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "UserImportJob": {
    "CloudWatchLogsRoleArn": "string",
    "CompletionDate": number,
    "CompletionMessage": "string",
    "CreationDate": number,
    "FailedUsers": number,
    "ImportedUsers": number,
    "JobId": "string",
    "JobName": "string",
    "PreSignedUrl": "string",
    "SkippedUsers": number,
    "StartDate": number,
    "Status": "string",
    "UserPoolId": "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.

UserImportJob

The details of the user import job. Includes logging destination, status, and the Amazon S3 pre-signed URL for CSV upload.

Type: [UserImportJobType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PreconditionNotMetException

This exception is thrown when a precondition is not met.

message

The message returned when a precondition is not met.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request starts the requested import job.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.StartUserImportJob
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "JobId": "import-mAgUtd8PMm",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
```

```
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "UserImportJob": {
    "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/example-cloudwatch-logs-role",
    "CreationDate": 1736442975.904,
    "FailedUsers": 0,
    "ImportedUsers": 0,
    "JobId": "import-mAgUtd8PMm",
    "JobName": "Customer import",
    "PreSignedUrl": "https://aws-cognito-idp-user-import-pdx.s3.us-west-2.amazonaws.com/123456789012/us-west-2_EXAMPLE/import-mAgUtd8PMm?X-Amz-Security-Token=[token]&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20241226T193341Z&X-Amz-SignedHeaders=host%3Bx-amz-server-side-encryption&X-Amz-Expires=899&X-Amz-Credential=[credential]&X-Amz-Signature=[signature]",
    "SkippedUsers": 0,
    "StartDate": 1736443020.081,
    "Status": "Pending",
    "UserPoolId": "us-west-2_EXAMPLE"
  }
}
```

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](#)

StartWebAuthnRegistration

Requests credential creation options from your user pool for the currently signed-in user. Returns information about the user pool, the user profile, and authentication requirements. Users must provide this information in their request to enroll your application with their passkey provider.

After users present this data and register with their passkey provider, return the response to your user pool in a [CompleteWebAuthnRegistration](#) API request.

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Request Syntax

```
{  
  "AccessToken": "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.

[AccessToken](#)

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: Yes

Response Syntax

```
{  
  "CredentialCreationOptions": JSON value  
}
```

```
}
```

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.

CredentialCreationOptions

The information that a user can provide in their request to register with their passkey provider.

Type: JSON value

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

WebAuthnConfigurationMissingException

This exception is thrown when a user pool doesn't have a configured relying party id or a user pool domain.

HTTP Status Code: 400

WebAuthnNotEnabledException

This exception is thrown when the passkey feature isn't enabled for the user pool.

HTTP Status Code: 400

Examples

Example

The following example request gets passkey registration options for the current user.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.StartWebAuthnRegistration
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
```

```
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "CredentialCreationOptions": {
    "authenticatorSelection": {
      "requireResidentKey": true,
      "residentKey": "required",
      "userVerification": "preferred"
    },
    "challenge": "wxvbDicyqQqvF2EXAMPLE",
    "excludeCredentials": [
      {
        "id": "8LApgk4-lNUFHbhm2w6Und7-uxcc8coJGsPxiogvHoItc64xWQc3r4CEXAMPLE",
        "type": "public-key"
      }
    ],
    "pubKeyCredParams": [
      {
        "alg": -7,
        "type": "public-key"
      },
      {
        "alg": -257,
        "type": "public-key"
      }
    ],
    "rp": {
      "id": "auth.example.com",
      "name": "auth.example.com"
    },
    "timeout": 60000,
    "user": {
      "displayName": "testuser",
      "id": "ZWfhZDAYMTktMjExNy00MzlmLTlkNDYtNGRiMjBlNEXAMPLE",
      "name": "testuser"
    }
  }
}
```

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](#)

StopUserImportJob

Instructs your user pool to stop a running job that's importing users from a CSV file that contains their usernames and attributes. For more information about importing users from a CSV file, see [Importing users from a CSV file](#).

To create a new import job, see [CreateUserImportJob](#). To generate a template for your import, see [GetCSVHeader](#).

Request Syntax

```
{  
  "JobId": "string",  
  "UserPoolId": "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.

[JobId](#)

The ID of a running user import job.

To get information about import jobs, see [ListUserImportJobs](#).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: import-[0-9a-zA-Z-]+

Required: Yes

[UserPoolId](#)

The ID of the user pool that you want to stop.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "UserImportJob": {
    "CloudWatchLogsRoleArn": "string",
    "CompletionDate": number,
    "CompletionMessage": "string",
    "CreationDate": number,
    "FailedUsers": number,
    "ImportedUsers": number,
    "JobId": "string",
    "JobName": "string",
    "PreSignedUrl": "string",
    "SkippedUsers": number,
    "StartDate": number,
    "Status": "string",
    "UserPoolId": "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.

UserImportJob

The details of the user import job. Includes logging destination, status, and the Amazon S3 pre-signed URL for CSV upload.

Type: [UserImportJobType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PreconditionNotMetException

This exception is thrown when a precondition is not met.

message

The message returned when a precondition is not met.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request stops the requested import job.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.StopUserImportJob
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "JobId": "import-mAgUtd8PMm",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
```

```
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "UserImportJob": {
    "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/example-cloudwatch-logs-role",
    "CompletionDate": 1736443496.379,
    "CompletionMessage": "The Import Job was stopped by the developer.",
    "CreationDate": 1736443471.781,
    "FailedUsers": 0,
    "ImportedUsers": 0,
    "JobId": "import-mAgUtd8PMm",
    "JobName": "Customer import",
    "PreSignedUrl": "https://aws-cognito-idp-user-import-pdx.s3.us-west-2.amazonaws.com/123456789012/us-west-2_EXAMPLE/import-mAgUtd8PMm?X-Amz-Security-Token=[token]&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20241226T193341Z&X-Amz-SignedHeaders=host%3Bx-amz-server-side-encryption&X-Amz-Expires=899&X-Amz-Credential=[credential]&X-Amz-Signature=[signature]",
    "SkippedUsers": 0,
    "StartDate": 1736443494.154,
    "Status": "Stopped",
    "UserPoolId": "us-west-2_EXAMPLE"
  }
}
```

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](#)

TagResource

Assigns a set of tags to an Amazon Cognito user pool. A tag is a label that you can use to categorize and manage user pools in different ways, such as by purpose, owner, environment, or other criteria.

Each tag consists of a key and value, both of which you define. A key is a general category for more specific values. For example, if you have two versions of a user pool, one for testing and another for production, you might assign an `Environment` tag key to both user pools. The value of this key might be `Test` for one user pool, and `Production` for the other.

Tags are useful for cost tracking and access control. You can activate your tags so that they appear on the Billing and Cost Management console, where you can track the costs associated with your user pools. In an AWS Identity and Access Management policy, you can constrain permissions for user pools based on specific tags or tag values.

You can use this action up to 5 times per second, per account. A user pool can have as many as 50 tags.

Request Syntax

```
{
  "ResourceArn": "string",
  "Tags": {
    "string" : "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.

ResourceArn

The Amazon Resource Name (ARN) of the user pool to assign the tags to.

Type: String

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

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

Required: Yes

Tags

An array of tag keys and values that you want to assign to the user pool.

Type: String to string map

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

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

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request adds administrator and tenant tags to the requested user pool.

Sample Request

```
POST HTTP/1.1
```



```
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.CognitoOperation
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ResourceArn": "arn:aws:cognito-idp:us-west-2:123456789012:userpool/us-
west-2_EXAMPLE",
  "Tags": {
    "administrator": "Jie",
    "tenant": "ExampleCorp"
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

UntagResource

Given tag IDs that you previously assigned to a user pool, removes them.

Request Syntax

```
{  
  "ResourceArn": "string",  
  "TagKeys": [ "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.

[ResourceArn](#)

The Amazon Resource Name (ARN) of the user pool that the tags are assigned to.

Type: String

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

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

Required: Yes

[TagKeys](#)

An array of tag keys that you want to remove from the user pool.

Type: Array of strings

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

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request removes the administrator and tenant tags from the requested user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.UntagResource
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ResourceArn": "arn:aws:cognito-idp:us-west-2:123456789012:userpool/us-
west-2_EXAMPLE",
  "TagKeys": [
    "administrator",
    "tenant"
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
```

```
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

UpdateAuthEventFeedback

Provides the feedback for an authentication event generated by threat protection features. The user's response indicates that you think that the event either was from a valid user or was an unwanted authentication attempt. This feedback improves the risk evaluation decision for the user pool as part of Amazon Cognito threat protection. To activate this setting, your user pool must be on the [Plus tier](#).

This operation requires a FeedbackToken that Amazon Cognito generates and adds to notification emails when users have potentially suspicious authentication events. Users invoke this operation when they select the link that corresponds to {one-click-link-valid} or {one-click-link-invalid} in your notification template. Because FeedbackToken is a required parameter, you can't make requests to UpdateAuthEventFeedback without the contents of the notification email message.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{
  "EventId": "string",
  "FeedbackToken": "string",
  "FeedbackValue": "string",
  "Username": "string",
  "UserPoolId": "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.

EventId

The ID of the authentication event that you want to submit feedback for.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 50.

Pattern: `[\w+ - ]+`

Required: Yes

FeedbackToken

The feedback token, an encrypted object generated by Amazon Cognito and passed to your user in the notification email message from the event.

Type: String

Pattern: `[A-Za-z0-9-_= . ]+`

Required: Yes

FeedbackValue

Your feedback to the authentication event. When you provide a `FeedbackValue` value of `valid`, you tell Amazon Cognito that you trust a user session where Amazon Cognito has evaluated some level of risk. When you provide a `FeedbackValue` value of `invalid`, you tell Amazon Cognito that you don't trust a user session, or you don't believe that Amazon Cognito evaluated a high-enough risk level.

Type: String

Valid Values: `Valid` | `Invalid`

Required: Yes

Username

The name of the user that you want to query or modify. The value of this parameter is typically your user's username, but it can be any of their alias attributes. If `username` isn't an alias attribute in your user pool, this value must be the sub of a local user or the username of a user from a third-party IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

UserPoolId

The ID of the user pool where you want to update auth event feedback.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

UserPoolAddOnNotEnabledException

This exception is thrown when user pool add-ons aren't enabled.

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](#)

UpdateDeviceStatus

Updates the status of a the currently signed-in user's device so that it is marked as remembered or not remembered for the purpose of device authentication. Device authentication is a "remember me" mechanism that silently completes sign-in from trusted devices with a device key instead of a user-provided MFA code. This operation changes the status of a device without deleting it, so you can enable it again later. For more information about device authentication, see [Working with devices](#).

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{
  "AccessToken": "string",
  "DeviceKey": "string",
  "DeviceRememberedStatus": "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.

AccessToken

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: Yes

DeviceKey

The device key of the device you want to update, for example `us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-f-]+`

Required: Yes

DeviceRememberedStatus

To enable device authentication with the specified device, set to `remembered`. To disable, set to `not_remembered`.

Type: String

Valid Values: `remembered` | `not_remembered`

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](#).

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request forgets a remembered device for the current user.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.UpdateDeviceStatus
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE",
  "DeviceKey": "us-west-2_a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "DeviceRememberedStatus": "not_remembered"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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](#)

UpdateGroup

Given the name of a user pool group, updates any of the properties for precedence, IAM role, or description. For more information about user pool groups, see [Adding groups to a user pool](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "Description": "string",
  "GroupName": "string",
  "Precedence": number,
  "RoleArn": "string",
  "UserPoolId": "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.

Description

A new description of the existing group.

Type: String

Length Constraints: Maximum length of 2048.

Required: No

GroupName

The name of the group that you want to update.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: Yes

Precedence

A non-negative integer value that specifies the precedence of this group relative to the other groups that a user can belong to in the user pool. Zero is the highest precedence value. Groups with lower Precedence values take precedence over groups with higher or null Precedence values. If a user belongs to two or more groups, it is the group with the lowest precedence value whose role ARN is given in the user's tokens for the `cognito:roles` and `cognito:preferred_role` claims.

Two groups can have the same Precedence value. If this happens, neither group takes precedence over the other. If two groups with the same Precedence have the same role ARN, that role is used in the `cognito:preferred_role` claim in tokens for users in each group. If the two groups have different role ARNs, the `cognito:preferred_role` claim isn't set in users' tokens.

The default Precedence value is null. The maximum Precedence value is $2^{31}-1$.

Type: Integer

Valid Range: Minimum value of 0.

Required: No

RoleArn

The Amazon Resource Name (ARN) of an IAM role that you want to associate with the group. The role assignment contributes to the `cognito:roles` and `cognito:preferred_role` claims in group members' tokens.

Type: String

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

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

Required: No

UserPoolId

The ID of the user pool that contains the group you want to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "Group": {
    "CreationDate": number,
    "Description": "string",
    "GroupName": "string",
    "LastModifiedDate": number,
    "Precedence": number,
    "RoleArn": "string",
    "UserPoolId": "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.

Group

Contains the updated details of the group, including precedence, IAM role, and description.

Type: [GroupType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request sets a description and IAM role for the requested group name.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.UpdateGroup
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "Description": "My example group",
  "GroupName": "testgroup",
  "Precedence": 4,
  "RoleArn": "arn:aws:iam::123456789012:role/example-group-role",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "Group": {
    "CreationDate": 1681422900.933,
    "Description": "My example group",
    "GroupName": "testgroup",
    "LastModifiedDate": 1736443988.896,
    "Precedence": 4,
    "RoleArn": "arn:aws:iam::123456789012:role/example-group-role",
    "UserPoolId": "us-west-2_EXAMPLE"
  }
}
```

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](#)

UpdateIdentityProvider

Modifies the configuration and trust relationship between a third-party identity provider (IdP) and a user pool. Amazon Cognito accepts sign-in with third-party identity providers through managed login and OIDC relying-party libraries. For more information, see [Third-party IdP sign-in](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "AttributeMapping": {
    "string" : "string"
  },
  "IdpIdentifiers": [ "string" ],
  "ProviderDetails": {
    "string" : "string"
  },
  "ProviderName": "string",
  "UserPoolId": "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.

AttributeMapping

A mapping of IdP attributes to standard and custom user pool attributes. Specify a user pool attribute as the key of the key-value pair, and the IdP attribute claim name as the value.

Type: String to string map

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

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

IdpIdentifiers

An array of IdP identifiers, for example "IdpIdentifiers": ["MyIdP", "MyIdP2"]. Identifiers are friendly names that you can pass in the `idp_identifier` query parameter of requests to the [Authorize endpoint](#) to silently redirect to sign-in with the associated IdP. Identifiers in a domain format also enable the use of [email-address matching with SAML providers](#).

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 40.

Pattern: [`\w\s+=. @- ]`+

Required: No

ProviderDetails

The scopes, URLs, and identifiers for your external identity provider. The following examples describe the provider detail keys for each IdP type. These values and their schema are subject to change. Social IdP `authorize_scopes` values must match the values listed here.

OpenID Connect (OIDC)

Amazon Cognito accepts the following elements when it can't discover endpoint URLs from `oidc_issuer`: `attributes_url`, `authorize_url`, `jwks_uri`, `token_url`.

```
Create or update request: "ProviderDetails": { "attributes_request_method":  
"GET", "attributes_url": "https://auth.example.com/userInfo",  
"authorize_scopes": "openid profile email", "authorize_url": "https://
```

```
auth.example.com/authorize", "client_id": "1example23456789",  
"client_secret": "provider-app-client-secret", "jwks_uri": "https://  
auth.example.com/.well-known/jwks.json", "oidc_issuer": "https://  
auth.example.com", "token_url": "https://example.com/token" }
```

```
Describe response: "ProviderDetails": { "attributes_request_method":  
"GET", "attributes_url": "https://auth.example.com/userInfo",  
"attributes_url_add_attributes": "false", "authorize_scopes": "openid  
profile email", "authorize_url": "https://auth.example.com/authorize",  
"client_id": "1example23456789", "client_secret": "provider-app-  
client-secret", "jwks_uri": "https://auth.example.com/.well-known/  
jwks.json", "oidc_issuer": "https://auth.example.com", "token_url":  
"https://example.com/token" }
```

SAML

```
Create or update request with Metadata URL: "ProviderDetails": { "IDPInit":  
"true", "IDPSignout": "true", "EncryptedResponses" : "true",  
"MetadataURL": "https://auth.example.com/sso/saml/metadata",  
"RequestSigningAlgorithm": "rsa-sha256" }
```

```
Create or update request with Metadata file: "ProviderDetails": { "IDPInit":  
"true", "IDPSignout": "true", "EncryptedResponses" : "true",  
"MetadataFile": "[metadata XML]", "RequestSigningAlgorithm": "rsa-  
sha256" }
```

The value of `MetadataFile` must be the plaintext metadata document with all quote (") characters escaped by backslashes.

```
Describe response: "ProviderDetails": { "IDPInit": "true", "IDPSignout":  
"true", "EncryptedResponses" : "true", "ActiveEncryptionCertificate":  
"[certificate]", "MetadataURL": "https://auth.example.com/  
sso/saml/metadata", "RequestSigningAlgorithm": "rsa-sha256",  
"SLORedirectBindingURI": "https://auth.example.com/slo/saml",  
"SSORedirectBindingURI": "https://auth.example.com/sso/saml" }
```

LoginWithAmazon

```
Create or update request: "ProviderDetails": { "authorize_scopes":  
"profile postal_code", "client_id": "amzn1.application-oa2-
```

```
client.1example23456789", "client_secret": "provider-app-client-secret"
```

```
Describe response: "ProviderDetails": { "attributes_url": "https://api.amazon.com/user/profile", "attributes_url_add_attributes": "false", "authorize_scopes": "profile postal_code", "authorize_url": "https://www.amazon.com/ap/oa", "client_id": "amzn1.application-oa2-client.1example23456789", "client_secret": "provider-app-client-secret", "token_request_method": "POST", "token_url": "https://api.amazon.com/auth/o2/token" }
```

Google

```
Create or update request: "ProviderDetails": { "authorize_scopes": "email profile openid", "client_id": "1example23456789.apps.googleusercontent.com", "client_secret": "provider-app-client-secret" }
```

```
Describe response: "ProviderDetails": { "attributes_url": "https://people.googleapis.com/v1/people/me?personFields=", "attributes_url_add_attributes": "true", "authorize_scopes": "email profile openid", "authorize_url": "https://accounts.google.com/o/oauth2/v2/auth", "client_id": "1example23456789.apps.googleusercontent.com", "client_secret": "provider-app-client-secret", "oidc_issuer": "https://accounts.google.com", "token_request_method": "POST", "token_url": "https://www.googleapis.com/oauth2/v4/token" }
```

SignInWithApple

```
Create or update request: "ProviderDetails": { "authorize_scopes": "email name", "client_id": "com.example.cognito", "private_key": "1EXAMPLE", "key_id": "2EXAMPLE", "team_id": "3EXAMPLE" }
```

```
Describe response: "ProviderDetails": { "attributes_url_add_attributes": "false", "authorize_scopes": "email name", "authorize_url": "https://appleid.apple.com/auth/authorize", "client_id": "com.example.cognito", "key_id": "1EXAMPLE", "oidc_issuer": "https://appleid.apple.com", "team_id": "2EXAMPLE", "token_request_method": "POST", "token_url": "https://appleid.apple.com/auth/token" }
```

Facebook

Create or update request: "ProviderDetails": { "api_version": "v17.0",
"authorize_scopes": "public_profile, email", "client_id":
"1example23456789", "client_secret": "provider-app-client-secret" }

Describe response: "ProviderDetails": { "api_version": "v17.0",
"attributes_url": "https://graph.facebook.com/v17.0/me?fields=",
"attributes_url_add_attributes": "true", "authorize_scopes":
"public_profile, email", "authorize_url": "https://www.facebook.com/
v17.0/dialog/oauth", "client_id": "1example23456789", "client_secret":
"provider-app-client-secret", "token_request_method": "GET",
"token_url": "https://graph.facebook.com/v17.0/oauth/access_token" }

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ProviderName

The name of the IdP that you want to update. You can pass the identity provider name in the `identity_provider` query parameter of requests to the [Authorize endpoint](#) to silently redirect to sign-in with the associated IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\p{Z}]+`

Required: Yes

UserPoolId

The Id of the user pool where you want to update your IdP.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "IdentityProvider": {
    "AttributeMapping": {
      "string" : "string"
    },
    "CreationDate": number,
    "IdpIdentifiers": [ "string" ],
    "LastModifiedDate": number,
    "ProviderDetails": {
      "string" : "string"
    },
    "ProviderName": "string",
    "ProviderType": "string",
    "UserPoolId": "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.

IdentityProvider

The identity provider details.

Type: [IdentityProviderType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnsupportedIdentityProviderException

This exception is thrown when the specified identifier isn't supported.

HTTP Status Code: 400

Examples

Example

The following example request updates an OIDC identity provider. Note that this request sets a manual configuration of the OIDC service endpoints. If the `oidc_issuer` URL has a `.well-known/openid-configuration` endpoint, you can specify `oidc_issuer` alone and auto-discover the remaining endpoints.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.UpdateIdentityProvider
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AttributeMapping": {
    "email": "idp_email",
    "email_verified": "idp_email_verified",
```

```
    "username": "sub"
  },
  "CreationDate": 1.701129701653E9,
  "IdpIdentifiers": [
    "corp",
    "dev"
  ],
  "LastModifiedDate": 1.701129701653E9,
  "ProviderDetails": {
    "attributes_request_method": "GET",
    "attributes_url": "https://example.com/userInfo",
    "attributes_url_add_attributes": "false",
    "authorize_scopes": "openid profile",
    "authorize_url": "https://example.com/authorize",
    "client_id": "idpexampleclient123",
    "client_secret": "idpexamplesecret456",
    "jwks_uri": "https://example.com/.well-known/jwks.json",
    "oidc_issuer": "https://example.com",
    "token_url": "https://example.com/token"
  },
  "ProviderName": "MyOIDCIdP",
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "IdentityProvider": {
    "AttributeMapping": {
      "email": "idp_email",
      "email_verified": "idp_email_verified",
      "username": "sub"
    },
    "CreationDate": 1.701129701.653,
    "IdpIdentifiers": [
      "corp",
      "dev"
    ]
  }
}
```



```
    ],
    "LastModifiedDate": 1736444278.211,
    "ProviderDetails": {
        "attributes_request_method": "GET",
        "attributes_url": "https://example.com/userInfo",
        "attributes_url_add_attributes": "false",
        "authorize_scopes": "openid profile",
        "authorize_url": "https://example.com/authorize",
        "client_id": "idpexampleclient123",
        "client_secret": "idpexamplesecret456",
        "jwks_uri": "https://example.com/.well-known/jwks.json",
        "oidc_issuer": "https://example.com",
        "token_url": "https://example.com/token"
    },
    "ProviderName": "MyOIDCIdP",
    "ProviderType": "OIDC",
    "UserPoolId": "us-west-2_EXAMPLE"
}
```

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](#)

UpdateManagedLoginBranding

Configures the branding settings for a user pool style. This operation is the programmatic option for the configuration of a style in the branding editor.

Provides values for UI customization in a Settings JSON object and image files in an Assets array.

This operation has a 2-megabyte request-size limit and include the CSS settings and image assets for your app client. Your branding settings might exceed 2MB in size. Amazon Cognito doesn't require that you pass all parameters in one request and preserves existing style settings that you don't specify. If your request is larger than 2MB, separate it into multiple requests, each with a size smaller than the limit.

As a best practice, modify the output of [DescribeManagedLoginBrandingByClient](#) into the request parameters for this operation. To get all settings, set ReturnMergedResources to true. For more information, see [API and SDK operations for managed login branding](#)

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "Assets": [
    {
      "Bytes": blob,
      "Category": "string",
      "ColorMode": "string",
      "Extension": "string",
      "ResourceId": "string"
```

```
    }  
  ],  
  "ManagedLoginBrandingId": "string",  
  "Settings": JSON value,  
  "UseCognitoProvidedValues": boolean,  
  "UserPoolId": "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.

[Assets](#)

An array of image files that you want to apply to roles like backgrounds, logos, and icons. Each object must also indicate whether it is for dark mode, light mode, or browser-adaptive mode.

Type: Array of [AssetType](#) objects

Array Members: Minimum number of 0 items. Maximum number of 40 items.

Required: No

[ManagedLoginBrandingId](#)

The ID of the managed login branding style that you want to update.

Type: String

Pattern: `^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[4][0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}$`

Required: No

[Settings](#)

A JSON file, encoded as a Document type, with the the settings that you want to apply to your style.

The following components are not currently implemented and reserved for future use:

- `signUp`
- `instructions`

- `sessionTimerDisplay`
- `languageSelector` (for localization, see [Managed login localization](#))

Type: JSON value

Required: No

[UseCognitoProvidedValues](#)

When `true`, applies the default branding style options. This option reverts to default style options that are managed by Amazon Cognito. You can modify them later in the branding editor.

When you specify `true` for this option, you must also omit values for `Settings` and `Assets` in the request.

Type: Boolean

Required: No

[UserPoolId](#)

The ID of the user pool that contains the managed login branding style that you want to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: No

Response Syntax

```
{
  "ManagedLoginBranding": {
    "Assets": [
      {
        "Bytes": blob,
        "Category": "string",
        "ColorMode": "string",
        "Extension": "string",
```

```
        "ResourceId": "string"
    }
],
"CreationDate": number,
"LastModifiedDate": number,
"ManagedLoginBrandingId": "string",
"Settings": JSON value,
"UseCognitoProvidedValues": boolean,
"UserPoolId": "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.

ManagedLoginBranding

The details of the branding style that you updated.

Type: [ManagedLoginBrandingType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example updates the branding configuration of the branding style with ID 63f30090-6b1f-4278-b885-2bbb81f8e545.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.ca-central-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.CreateManagedLoginBranding
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "Assets": [
    {
      "Bytes":
        "PHN2ZyB3aWR0aD0iMjAwMDAiIGhlaWdodD0iNDAwIiB2aWV3Qm94PSIwIDAgMjAwMDAgNDAwIiBmaWxsPSJub251IiB4b
        +CjxyZWNoIHdpZHRoPSIyMDAwMCIgaGVpZ2h0PSI0MDAiIGZpbGw9InVybCgjcGFpbnQwX2xpbmVhcl8xNzI1OV8yMzY2Nz
        +CjxsaW51YXJHcmFkaWVudCBpZD0icGFpbnQwX2xpbmVhcl8xNzI1OV8yMzY2NzQiIHgxPSItODk0LjI0OSIgeTE9IjE5OS
        +Cjwvc3ZnPg0=",
      "Category": "PAGE_FOOTER_BACKGROUND",
      "ColorMode": "DARK",
      "Extension": "SVG"
    }
  ],
  "ManagedLoginBrandingId": "63f30090-6b1f-4278-b885-2bbb81f8e545",
  "Settings": {
    "categories": {
      "auth": {
        "authMethodOrder": [
          {
            "display": "BUTTON",
            "type": "FEDERATED"
          }
        ]
      }
    }
  }
}
```

```
        {
            "display": "INPUT",
            "type": "USERNAME_PASSWORD"
        }
    ],
    "federation": {
        "interfaceStyle": "BUTTON_LIST",
        "order": [
        ]
    }
},
"form": {
    "displayGraphics": true,
    "instructions": {
        "enabled": false
    },
    "languageSelector": {
        "enabled": false
    },
    "location": {
        "horizontal": "CENTER",
        "vertical": "CENTER"
    },
    "sessionTimerDisplay": "NONE"
},
"global": {
    "colorSchemeMode": "LIGHT",
    "pageFooter": {
        "enabled": false
    },
    "pageHeader": {
        "enabled": false
    },
    "spacingDensity": "REGULAR"
},
"signUp": {
    "acceptanceElements": [
        {
            "enforcement": "NONE",
            "textKey": "en"
        }
    ]
}
```



```
    },
    "componentClasses": {
      "buttons": {
        "borderRadius": 8.0
      },
      "divider": {
        "darkMode": {
          "borderColor": "232b37ff"
        },
        "lightMode": {
          "borderColor": "ebebff"
        }
      },
      "dropDown": {
        "borderRadius": 8.0,
        "darkMode": {
          "defaults": {
            "itemBackgroundColor": "192534ff"
          },
          "hover": {
            "itemBackgroundColor": "081120ff",
            "itemBorderColor": "5f6b7aff",
            "itemTextColor": "e9ebedff"
          },
          "match": {
            "itemBackgroundColor": "d1d5dbff",
            "itemTextColor": "89bdeeff"
          }
        },
        "lightMode": {
          "defaults": {
            "itemBackgroundColor": "ffffffff"
          },
          "hover": {
            "itemBackgroundColor": "f4f4f4ff",
            "itemBorderColor": "7d8998ff",
            "itemTextColor": "000716ff"
          },
          "match": {
            "itemBackgroundColor": "414d5cff",
            "itemTextColor": "0972d3ff"
          }
        }
      }
    },
  },
```

```
"focusState": {
  "darkMode": {
    "borderColor": "539fe5ff"
  },
  "lightMode": {
    "borderColor": "0972d3ff"
  }
},
"idpButtons": {
  "icons": {
    "enabled": true
  }
},
"input": {
  "borderRadius": 8.0,
  "darkMode": {
    "defaults": {
      "backgroundColor": "0f1b2aff",
      "borderColor": "5f6b7aff"
    },
    "placeholderColor": "8d99a8ff"
  },
  "lightMode": {
    "defaults": {
      "backgroundColor": "ffffffff",
      "borderColor": "7d8998ff"
    },
    "placeholderColor": "5f6b7aff"
  }
},
"inputDescription": {
  "darkMode": {
    "textColor": "8d99a8ff"
  },
  "lightMode": {
    "textColor": "5f6b7aff"
  }
},
"inputLabel": {
  "darkMode": {
    "textColor": "d1d5dbff"
  },
  "lightMode": {
    "textColor": "000716ff"
  }
}
```

```
    }
  },
  "link": {
    "darkMode": {
      "defaults": {
        "textColor": "539fe5ff"
      },
      "hover": {
        "textColor": "89bdeeff"
      }
    },
    "lightMode": {
      "defaults": {
        "textColor": "0972d3ff"
      },
      "hover": {
        "textColor": "033160ff"
      }
    }
  },
  "optionControls": {
    "darkMode": {
      "defaults": {
        "backgroundColor": "0f1b2aff",
        "borderColor": "7d8998ff"
      },
      "selected": {
        "backgroundColor": "539fe5ff",
        "foregroundColor": "000716ff"
      }
    },
    "lightMode": {
      "defaults": {
        "backgroundColor": "ffffffff",
        "borderColor": "7d8998ff"
      },
      "selected": {
        "backgroundColor": "0972d3ff",
        "foregroundColor": "ffffffff"
      }
    }
  },
  "statusIndicator": {
    "darkMode": {
```

```
        "error": {
            "backgroundColor": "1a0000ff",
            "borderColor": "eb6f6fff",
            "indicatorColor": "eb6f6fff"
        },
        "pending": {
            "indicatorColor": "AAAAAAAA"
        },
        "success": {
            "backgroundColor": "001a02ff",
            "borderColor": "29ad32ff",
            "indicatorColor": "29ad32ff"
        },
        "warning": {
            "backgroundColor": "1d1906ff",
            "borderColor": "e0ca57ff",
            "indicatorColor": "e0ca57ff"
        }
    },
    "lightMode": {
        "error": {
            "backgroundColor": "fff7f7ff",
            "borderColor": "d91515ff",
            "indicatorColor": "d91515ff"
        },
        "pending": {
            "indicatorColor": "AAAAAAAA"
        },
        "success": {
            "backgroundColor": "f2fcf3ff",
            "borderColor": "037f0cff",
            "indicatorColor": "037f0cff"
        },
        "warning": {
            "backgroundColor": "fffce9ff",
            "borderColor": "8d6605ff",
            "indicatorColor": "8d6605ff"
        }
    }
},
"components": {
    "alert": {
        "borderRadius": 12.0,
```

```
    "darkMode": {
      "error": {
        "backgroundColor": "1a0000ff",
        "borderColor": "eb6f6fff"
      }
    },
    "lightMode": {
      "error": {
        "backgroundColor": "fff7f7ff",
        "borderColor": "d91515ff"
      }
    }
  },
  "favicon": {
    "enabledTypes": [
      "ICO",
      "SVG"
    ]
  },
  "form": {
    "backgroundImage": {
      "enabled": false
    },
    "borderRadius": 8.0,
    "darkMode": {
      "backgroundColor": "0f1b2aff",
      "borderColor": "424650ff"
    },
    "lightMode": {
      "backgroundColor": "ffffffff",
      "borderColor": "c6c6cdff"
    },
    "logo": {
      "enabled": false,
      "formInclusion": "IN",
      "location": "CENTER",
      "position": "TOP"
    }
  },
  "idpButton": {
    "custom": {
    },
    "standard": {
      "darkMode": {
```

```

        "active": {
            "backgroundColor": "354150ff",
            "borderColor": "89bdeeff",
            "textColor": "89bdeeff"
        },
        "defaults": {
            "backgroundColor": "0f1b2aff",
            "borderColor": "c6c6cdff",
            "textColor": "c6c6cdff"
        },
        "hover": {
            "backgroundColor": "192534ff",
            "borderColor": "89bdeeff",
            "textColor": "89bdeeff"
        }
    },
    "lightMode": {
        "active": {
            "backgroundColor": "d3e7f9ff",
            "borderColor": "033160ff",
            "textColor": "033160ff"
        },
        "defaults": {
            "backgroundColor": "ffffffff",
            "borderColor": "424650ff",
            "textColor": "424650ff"
        },
        "hover": {
            "backgroundColor": "f2f8fdff",
            "borderColor": "033160ff",
            "textColor": "033160ff"
        }
    }
},
"pageBackground": {
    "darkMode": {
        "color": "0f1b2aff"
    },
    "image": {
        "enabled": true
    },
    "lightMode": {
        "color": "ffffffff"
    }
}

```

```
    }
  },
  "pageFooter": {
    "backgroundImage": {
      "enabled": false
    },
    "darkMode": {
      "background": {
        "color": "0f141aff"
      },
      "borderColor": "424650ff"
    },
    "lightMode": {
      "background": {
        "color": "fafafaff"
      },
      "borderColor": "d5dbdbff"
    },
    "logo": {
      "enabled": false,
      "location": "START"
    }
  },
  "pageHeader": {
    "backgroundImage": {
      "enabled": false
    },
    "darkMode": {
      "background": {
        "color": "0f141aff"
      },
      "borderColor": "424650ff"
    },
    "lightMode": {
      "background": {
        "color": "fafafaff"
      },
      "borderColor": "d5dbdbff"
    },
    "logo": {
      "enabled": false,
      "location": "START"
    }
  },
}
```

```
"pageText": {
  "darkMode": {
    "bodyColor": "b6bec9ff",
    "descriptionColor": "b6bec9ff",
    "headingColor": "d1d5dbff"
  },
  "lightMode": {
    "bodyColor": "414d5cff",
    "descriptionColor": "414d5cff",
    "headingColor": "000716ff"
  }
},
"phoneNumberSelector": {
  "displayType": "TEXT"
},
"primaryButton": {
  "darkMode": {
    "active": {
      "backgroundColor": "539fe5ff",
      "textColor": "000716ff"
    },
    "defaults": {
      "backgroundColor": "539fe5ff",
      "textColor": "000716ff"
    },
    "disabled": {
      "backgroundColor": "ffffffff",
      "borderColor": "ffffffff"
    },
    "hover": {
      "backgroundColor": "89bdeeff",
      "textColor": "000716ff"
    }
  },
  "lightMode": {
    "active": {
      "backgroundColor": "033160ff",
      "textColor": "ffffffff"
    },
    "defaults": {
      "backgroundColor": "0972d3ff",
      "textColor": "ffffffff"
    },
    "disabled": {
```



```
        "backgroundColor": "ffffffff",
        "borderColor": "ffffffff"
    },
    "hover": {
        "backgroundColor": "033160ff",
        "textColor": "ffffffff"
    }
},
"secondaryButton": {
    "darkMode": {
        "active": {
            "backgroundColor": "354150ff",
            "borderColor": "89bdeeff",
            "textColor": "89bdeeff"
        },
        "defaults": {
            "backgroundColor": "0f1b2aff",
            "borderColor": "539fe5ff",
            "textColor": "539fe5ff"
        },
        "hover": {
            "backgroundColor": "192534ff",
            "borderColor": "89bdeeff",
            "textColor": "89bdeeff"
        }
    },
    "lightMode": {
        "active": {
            "backgroundColor": "d3e7f9ff",
            "borderColor": "033160ff",
            "textColor": "033160ff"
        },
        "defaults": {
            "backgroundColor": "ffffffff",
            "borderColor": "0972d3ff",
            "textColor": "0972d3ff"
        },
        "hover": {
            "backgroundColor": "f2f8fdff",
            "borderColor": "033160ff",
            "textColor": "033160ff"
        }
    }
}
```

```

    }
  }
},
"UseCognitoProvidedValues": false,
"UserPoolId": "ca-central-1_EXAMPLE"
}

```

Sample Response

```

HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "ManagedLoginBranding": {
    "Assets": [
      {
        "Bytes":
"PHN2ZyB3aWR0aD0iMjAwMDAiIGhlaWdodD0iNDAwIiB2aWV3Qm94PSIwIDAgMjAwMDAgNDAwIiBmaWxsPSJub251IiB4b
+CjxyZWNoIHdpZHRoPSIyMDAwMCIgaGVpZ2h0PSI0MDAiIGZpbGw9InVybcGjcGFpbnQwX2xpbmVhcl8xNzI1OV8yMzY2Nz
+CjxsaW51YXJHcmFkaWVudCBpZD0icGFpbnQwX2xpbmVhcl8xNzI1OV8yMzY2NzQiIHgPSItODk0LjI0OSIgeTE9IjE5OS
+Cjwvc3ZnPgo=",
        "Category": "PAGE_FOOTER_BACKGROUND",
        "ColorMode": "DARK",
        "Extension": "SVG"
      }
    ],
    "CreationDate": 1732138490.642,
    "LastModifiedDate": 1732140420.301,
    "ManagedLoginBrandingId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Settings": {
      "categories": {
        "auth": {
          "authMethodOrder": [
            {
              "display": "BUTTON",
              "type": "FEDERATED"
            }
          ],

```

```
        {
            "display": "INPUT",
            "type": "USERNAME_PASSWORD"
        }
    ],
    "federation": {
        "interfaceStyle": "BUTTON_LIST",
        "order": [
        ]
    }
},
"form": {
    "displayGraphics": true,
    "instructions": {
        "enabled": false
    },
    "languageSelector": {
        "enabled": false
    },
    "location": {
        "horizontal": "CENTER",
        "vertical": "CENTER"
    },
    "sessionTimerDisplay": "NONE"
},
"global": {
    "colorSchemeMode": "LIGHT",
    "pageFooter": {
        "enabled": false
    },
    "pageHeader": {
        "enabled": false
    },
    "spacingDensity": "REGULAR"
},
"signUp": {
    "acceptanceElements": [
        {
            "enforcement": "NONE",
            "textKey": "en"
        }
    ]
}
```

```
    },
    "componentClasses": {
      "buttons": {
        "borderRadius": 8.0
      },
      "divider": {
        "darkMode": {
          "borderColor": "232b37ff"
        },
        "lightMode": {
          "borderColor": "ebbf0fff"
        }
      },
      "dropDown": {
        "borderRadius": 8.0,
        "darkMode": {
          "defaults": {
            "itemBackgroundColor": "192534ff"
          },
          "hover": {
            "itemBackgroundColor": "081120ff",
            "itemBorderColor": "5f6b7aff",
            "itemTextColor": "e9ebedff"
          },
          "match": {
            "itemBackgroundColor": "d1d5dbff",
            "itemTextColor": "89bdeeff"
          }
        },
        "lightMode": {
          "defaults": {
            "itemBackgroundColor": "ffffffff"
          },
          "hover": {
            "itemBackgroundColor": "f4f4f4ff",
            "itemBorderColor": "7d8998ff",
            "itemTextColor": "000716ff"
          },
          "match": {
            "itemBackgroundColor": "414d5cff",
            "itemTextColor": "0972d3ff"
          }
        }
      }
    },
  },
```

```
"focusState": {
  "darkMode": {
    "borderColor": "539fe5ff"
  },
  "lightMode": {
    "borderColor": "0972d3ff"
  }
},
"idpButtons": {
  "icons": {
    "enabled": true
  }
},
"input": {
  "borderRadius": 8.0,
  "darkMode": {
    "defaults": {
      "backgroundColor": "0f1b2aff",
      "borderColor": "5f6b7aff"
    },
    "placeholderColor": "8d99a8ff"
  },
  "lightMode": {
    "defaults": {
      "backgroundColor": "ffffffff",
      "borderColor": "7d8998ff"
    },
    "placeholderColor": "5f6b7aff"
  }
},
"inputDescription": {
  "darkMode": {
    "textColor": "8d99a8ff"
  },
  "lightMode": {
    "textColor": "5f6b7aff"
  }
},
"inputLabel": {
  "darkMode": {
    "textColor": "d1d5dbff"
  },
  "lightMode": {
    "textColor": "000716ff"
  }
}
```

```
    }
  },
  "link": {
    "darkMode": {
      "defaults": {
        "textColor": "539fe5ff"
      },
      "hover": {
        "textColor": "89bdeeff"
      }
    },
    "lightMode": {
      "defaults": {
        "textColor": "0972d3ff"
      },
      "hover": {
        "textColor": "033160ff"
      }
    }
  },
  "optionControls": {
    "darkMode": {
      "defaults": {
        "backgroundColor": "0f1b2aff",
        "borderColor": "7d8998ff"
      },
      "selected": {
        "backgroundColor": "539fe5ff",
        "foregroundColor": "000716ff"
      }
    },
    "lightMode": {
      "defaults": {
        "backgroundColor": "ffffffff",
        "borderColor": "7d8998ff"
      },
      "selected": {
        "backgroundColor": "0972d3ff",
        "foregroundColor": "ffffffff"
      }
    }
  },
  "statusIndicator": {
    "darkMode": {
```

```

        "error": {
            "backgroundColor": "1a0000ff",
            "borderColor": "eb6f6fff",
            "indicatorColor": "eb6f6fff"
        },
        "pending": {
            "indicatorColor": "AAAAAAAA"
        },
        "success": {
            "backgroundColor": "001a02ff",
            "borderColor": "29ad32ff",
            "indicatorColor": "29ad32ff"
        },
        "warning": {
            "backgroundColor": "1d1906ff",
            "borderColor": "e0ca57ff",
            "indicatorColor": "e0ca57ff"
        }
    },
    "lightMode": {
        "error": {
            "backgroundColor": "fff7f7ff",
            "borderColor": "d91515ff",
            "indicatorColor": "d91515ff"
        },
        "pending": {
            "indicatorColor": "AAAAAAAA"
        },
        "success": {
            "backgroundColor": "f2fcf3ff",
            "borderColor": "037f0cff",
            "indicatorColor": "037f0cff"
        },
        "warning": {
            "backgroundColor": "fffce9ff",
            "borderColor": "8d6605ff",
            "indicatorColor": "8d6605ff"
        }
    }
},
"components": {
    "alert": {
        "borderRadius": 12.0,

```

```
    "darkMode": {
      "error": {
        "backgroundColor": "1a0000ff",
        "borderColor": "eb6f6fff"
      }
    },
    "lightMode": {
      "error": {
        "backgroundColor": "fff7f7ff",
        "borderColor": "d91515ff"
      }
    }
  },
  "favicon": {
    "enabledTypes": [
      "ICO",
      "SVG"
    ]
  },
  "form": {
    "backgroundImage": {
      "enabled": false
    },
    "borderRadius": 8.0,
    "darkMode": {
      "backgroundColor": "0f1b2aff",
      "borderColor": "424650ff"
    },
    "lightMode": {
      "backgroundColor": "ffffffff",
      "borderColor": "c6c6cdff"
    },
    "logo": {
      "enabled": false,
      "formInclusion": "IN",
      "location": "CENTER",
      "position": "TOP"
    }
  },
  "idpButton": {
    "custom": {
    },
    "standard": {
      "darkMode": {
```



```
        "active": {
            "backgroundColor": "354150ff",
            "borderColor": "89bdeeff",
            "textColor": "89bdeeff"
        },
        "defaults": {
            "backgroundColor": "0f1b2aff",
            "borderColor": "c6c6cdff",
            "textColor": "c6c6cdff"
        },
        "hover": {
            "backgroundColor": "192534ff",
            "borderColor": "89bdeeff",
            "textColor": "89bdeeff"
        }
    },
    "lightMode": {
        "active": {
            "backgroundColor": "d3e7f9ff",
            "borderColor": "033160ff",
            "textColor": "033160ff"
        },
        "defaults": {
            "backgroundColor": "ffffffff",
            "borderColor": "424650ff",
            "textColor": "424650ff"
        },
        "hover": {
            "backgroundColor": "f2f8fdff",
            "borderColor": "033160ff",
            "textColor": "033160ff"
        }
    }
},
"pageBackground": {
    "darkMode": {
        "color": "0f1b2aff"
    },
    "image": {
        "enabled": true
    },
    "lightMode": {
        "color": "ffffffff"
    }
}
```

```
    }
  },
  "pageFooter": {
    "backgroundImage": {
      "enabled": false
    },
    "darkMode": {
      "background": {
        "color": "0f141aff"
      },
      "borderColor": "424650ff"
    },
    "lightMode": {
      "background": {
        "color": "fafafaff"
      },
      "borderColor": "d5dbdbff"
    },
    "logo": {
      "enabled": false,
      "location": "START"
    }
  },
  "pageHeader": {
    "backgroundImage": {
      "enabled": false
    },
    "darkMode": {
      "background": {
        "color": "0f141aff"
      },
      "borderColor": "424650ff"
    },
    "lightMode": {
      "background": {
        "color": "fafafaff"
      },
      "borderColor": "d5dbdbff"
    },
    "logo": {
      "enabled": false,
      "location": "START"
    }
  },
}
```

```
"pageText": {
  "darkMode": {
    "bodyColor": "b6bec9ff",
    "descriptionColor": "b6bec9ff",
    "headingColor": "d1d5dbff"
  },
  "lightMode": {
    "bodyColor": "414d5cff",
    "descriptionColor": "414d5cff",
    "headingColor": "000716ff"
  }
},
"phoneNumberSelector": {
  "displayType": "TEXT"
},
"primaryButton": {
  "darkMode": {
    "active": {
      "backgroundColor": "539fe5ff",
      "textColor": "000716ff"
    },
    "defaults": {
      "backgroundColor": "539fe5ff",
      "textColor": "000716ff"
    },
    "disabled": {
      "backgroundColor": "ffffffff",
      "borderColor": "ffffffff"
    },
    "hover": {
      "backgroundColor": "89bdeeff",
      "textColor": "000716ff"
    }
  },
  "lightMode": {
    "active": {
      "backgroundColor": "033160ff",
      "textColor": "ffffffff"
    },
    "defaults": {
      "backgroundColor": "0972d3ff",
      "textColor": "ffffffff"
    },
    "disabled": {
```

```
        "backgroundColor": "ffffffff",
        "borderColor": "ffffffff"
    },
    "hover": {
        "backgroundColor": "033160ff",
        "textColor": "ffffffff"
    }
},
"secondaryButton": {
    "darkMode": {
        "active": {
            "backgroundColor": "354150ff",
            "borderColor": "89bdeeff",
            "textColor": "89bdeeff"
        },
        "defaults": {
            "backgroundColor": "0f1b2aff",
            "borderColor": "539fe5ff",
            "textColor": "539fe5ff"
        },
        "hover": {
            "backgroundColor": "192534ff",
            "borderColor": "89bdeeff",
            "textColor": "89bdeeff"
        }
    },
    "lightMode": {
        "active": {
            "backgroundColor": "d3e7f9ff",
            "borderColor": "033160ff",
            "textColor": "033160ff"
        },
        "defaults": {
            "backgroundColor": "ffffffff",
            "borderColor": "0972d3ff",
            "textColor": "0972d3ff"
        },
        "hover": {
            "backgroundColor": "f2f8fdff",
            "borderColor": "033160ff",
            "textColor": "033160ff"
        }
    }
}
```

```
        }
    },
    "UseCognitoProvidedValues": false,
    "UserPoolId": "ca-central-1_EXAMPLE"
}
```

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](#)

UpdateResourceServer

Updates the name and scopes of a resource server. All other fields are read-only. For more information about resource servers, see [Access control with resource servers](#).

Important

If you don't provide a value for an attribute, it is set to the default value.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "Identifier": "string",
  "Name": "string",
  "Scopes": [
    {
      "ScopeDescription": "string",
      "ScopeName": "string"
    }
  ],
  "UserPoolId": "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.

Identifier

A unique resource server identifier for the resource server. The identifier can be an API friendly name like `solar-system-data`. You can also set an API URL like `https://solar-system-data-api.example.com` as your identifier.

Amazon Cognito represents scopes in the access token in the format `$resource-server-identifier/$scope`. Longer scope-identifier strings increase the size of your access tokens.

Type: String

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

Pattern: `[\x21\x23-\x5B\x5D-\x7E]+`

Required: Yes

Name

The updated name of the resource server.

Type: String

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

Pattern: `[\w\s+=, .@- ]+`

Required: Yes

Scopes

An array of updated custom scope names and descriptions that you want to associate with your resource server.

Type: Array of [ResourceServerScopeType](#) objects

Array Members: Maximum number of 100 items.

Required: No

UserPoolId

The ID of the user pool that contains the resource server that you want to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "ResourceServer": {
    "Identifier": "string",
    "Name": "string",
    "Scopes": [
      {
        "ScopeDescription": "string",
        "ScopeName": "string"
      }
    ],
    "UserPoolId": "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.

ResourceServer

The updated details of the requested resource server.

Type: [ResourceServerType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request adds two scopes to the requested resource server.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.UpdateResourceServer
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "Identifier": "myapi.example.com",
  "Name": "Example API with custom access control scopes",
  "Scopes": [
    {
      "ScopeDescription": "International customers",
      "ScopeName": "international.read"
    },
    {
      "ScopeDescription": "Domestic customers",
      "ScopeName": "domestic.read"
    }
  ],
  "UserPoolId": "us-west-2_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
```

```
Connection: keep-alive
{
  "ResourceServer": {
    "Identifier": "myapi.example.com",
    "Name": "Example API with custom access control scopes",
    "Scopes": [
      {
        "ScopeDescription": "International customers",
        "ScopeName": "international.read"
      },
      {
        "ScopeDescription": "Domestic customers",
        "ScopeName": "domestic.read"
      }
    ],
    "UserPoolId": "us-west-2_EXAMPLE"
  }
}
```

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](#)

UpdateTerms

Modifies existing terms documents for the requested app client. When Terms and conditions and Privacy policy documents are configured, the app client displays links to them in the sign-up page of managed login for the app client.

You can provide URLs for terms documents in the languages that are supported by [managed login localization](#). Amazon Cognito directs users to the terms documents for their current language, with fallback to default if no document exists for the language.

Each request accepts one type of terms document and a map of language-to-link for that document type. You must provide both types of terms documents in at least one language before Amazon Cognito displays your terms documents. Supply each type in separate requests.

For more information, see [Terms documents](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "Enforcement": "string",
  "Links": {
    "string" : "string"
  },
  "TermsId": "string",
  "TermsName": "string",
  "TermsSource": "string",
  "UserPoolId": "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.

[Enforcement](#)

This parameter is reserved for future use and currently accepts only one value.

Type: String

Valid Values: NONE

Required: No

[Links](#)

A map of URLs to languages. For each localized language that will view the requested TermsName, assign a URL. A selection of `cognito:default` displays for all languages that don't have a language-specific URL.

For example, `"cognito:default": "https://terms.example.com"`,
`"cognito:spanish": "https://terms.example.com/es"`.

Type: String to string map

Map Entries: Maximum number of 12 items.

Key Pattern: `^cognito:(default|english|french|spanish|german|bahasa-indonesia|italian|japanese|korean|portuguese-brazil|chinese-(simplified|traditional))$`

Value Length Constraints: Minimum length of 1. Maximum length of 1024.

Value Pattern: `^[\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}]+$`

Required: No

[TermsId](#)

The ID of the terms document that you want to update.

Retrieve terms IDs with [DescribeTerms](#) or [ListTerms](#).

Type: String

Pattern: `^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[4][0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}$`

Required: Yes

TermsName

The new name that you want to apply to the requested terms documents.

Type: String

Pattern: `^(terms-of-use|privacy-policy)$`

Required: No

TermsSource

This parameter is reserved for future use and currently accepts only one value.

Type: String

Valid Values: LINK

Required: No

UserPoolId

The ID of the user pool that contains the terms that you want to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{  
  "Terms": {
```

```
"ClientId": "string",
"CreationDate": number,
"Enforcement": "string",
"LastModifiedDate": number,
"Links": {
  "string" : "string"
},
"TermsId": "string",
"TermsName": "string",
"TermsSource": "string",
"UserPoolId": "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.

[Terms](#)

A summary of the updates to your terms documents.

Type: [TermsType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TermsExistsException

Terms document names must be unique to the app client. This exception is thrown when you attempt to create terms documents with a duplicate `TermsName`.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example operation updates a privacy policy terms document to add a Japanese language URL.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.UpdateTerms
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>

{
  "TermsId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Enforcement": "NONE",
  "Links": {
    "cognito:default": "https://example.com/privacy/",
    "cognito:french": "https://example.com/fr/privacy/",
    "cognito:portuguese-brazil": "https://example.com/pt/privacy/",
    "cognito:japanese": "https://example.com/ja-JP/privacy"
  },
  "TermsName": "privacy-policy",
  "TermsSource": "LINK",
  "UserPoolId": "us-east-1_EXAMPLE"
```

```
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive

{
  "Terms": {
    "ClientId": "1example23456789",
    "CreationDate": 1755798239.324,
    "Enforcement": "NONE",
    "LastModifiedDate": 1755798384.223,
    "Links": {
      "cognito:default": "https://example.com/privacy/",
      "cognito:french": "https://example.com/fr/privacy",
      "cognito:portuguese-brazil": "https://example.com/pt/privacy/",
      "cognito:japanese": "https://example.com/ja-JP/privacy"
    },
    "TermsId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "TermsName": "privacy-policy",
    "TermsSource": "LINK",
    "UserPoolId": "us-east-1_EXAMPLE"
  }
}
```

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](#)

UpdateUserAttributes

Updates the currently signed-in user's attributes. To delete an attribute from the user, submit the attribute in your API request with a blank value.

For custom attributes, you must add a `custom:` prefix to the attribute name, for example `custom:department`.

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Request Syntax

```
{
  "AccessToken": "string",
  "ClientMetadata": {
    "string" : "string"
  },
  "UserAttributes": [
    {
      "Name": "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.

[AccessToken](#)

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws.cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: Yes

[ClientMetadata](#)

A map of custom key-value pairs that you can provide as input for any custom workflows that this action triggers. You create custom workflows by assigning AWS Lambda functions to user pool triggers.

When Amazon Cognito invokes any of these functions, it passes a JSON payload, which the function receives as input. This payload contains a `clientMetadata` attribute that provides the data that you assigned to the `ClientMetadata` parameter in your request. In your function

code, you can process the `clientMetadata` value to enhance your workflow for your specific needs.

To review the Lambda trigger types that Amazon Cognito invokes at runtime with API requests, see [Connecting API actions to Lambda triggers](#) in the *Amazon Cognito Developer Guide*.

 Note

When you use the `ClientMetadata` parameter, note that Amazon Cognito won't do the following:

- Store the `ClientMetadata` value. This data is available only to AWS Lambda triggers that are assigned to a user pool to support custom workflows. If your user pool configuration doesn't include triggers, the `ClientMetadata` parameter serves no purpose.
- Validate the `ClientMetadata` value.
- Encrypt the `ClientMetadata` value. Don't send sensitive information in this parameter.

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

UserAttributes

An array of name-value pairs representing user attributes.

For custom attributes, you must add a `custom:` prefix to the attribute name.

If you have set an attribute to require verification before Amazon Cognito updates its value, this request doesn't immediately update the value of that attribute. After your user receives and responds to a verification message to verify the new value, Amazon Cognito updates the attribute value. Your user can sign in and receive messages with the original attribute value until they verify the new value.

Type: Array of [AttributeType](#) objects

Required: Yes

Response Syntax

```
{
  "CodeDeliveryDetailsList": [
    {
      "AttributeName": "string",
      "DeliveryMedium": "string",
      "Destination": "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.

[CodeDeliveryDetailsList](#)

When the attribute-update request includes an email address or phone number attribute, Amazon Cognito sends a message to users with a code that confirms ownership of the new value that they entered. The `CodeDeliveryDetails` object is information about the delivery destination for that link or code. This behavior happens in user pools configured to automatically verify changes to those attributes. For more information, see [Verifying when users change their email or phone number](#).

Type: Array of [CodeDeliveryDetailsType](#) objects

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

AliasExistsException

This exception is thrown when a user tries to confirm the account with an email address or phone number that has already been supplied as an alias for a different user profile. This

exception indicates that an account with this email address or phone already exists in a user pool that you've configured to use email address or phone number as a sign-in alias.

message

The message that Amazon Cognito sends to the user when the value of an alias attribute is already linked to another user profile.

HTTP Status Code: 400

CodeDeliveryFailureException

This exception is thrown when a verification code fails to deliver successfully.

message

The message sent when a verification code fails to deliver successfully.

HTTP Status Code: 400

CodeMismatchException

This exception is thrown if the provided code doesn't match what the server was expecting.

message

The message provided when the code mismatch exception is thrown.

HTTP Status Code: 400

ExpiredCodeException

This exception is thrown if a code has expired.

message

The message returned when the expired code exception is thrown.

HTTP Status Code: 400

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidLambdaResponseException

This exception is thrown when Amazon Cognito encounters an invalid AWS Lambda response.

message

The message returned when Amazon Cognito throws an invalid AWS Lambda response exception.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UnexpectedLambdaException

This exception is thrown when Amazon Cognito encounters an unexpected exception with AWS Lambda.

message

The message returned when Amazon Cognito returns an unexpected Lambda exception.

HTTP Status Code: 400

UserLambdaValidationException

This exception is thrown when the Amazon Cognito service encounters a user validation exception with the AWS Lambda service.

message

The message returned when the Amazon Cognito service returns a user validation exception with the Lambda service.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request updates several attributes for the current user. The change to the user's email address generates a verification code that the user can provide in a `VerifyUserAttributes` request.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.UpdateUserAttributes
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE",
  "UserAttributes": [
    {
      "Name": "email",
      "Value": "johndoe@example.com"
    },
    {
      "Name": "birthdate",
      "Value": "01/01/2025"
    },
    {
```

```
        "Name": "custom:costcenter",
        "Value": "mycustomvalue"
    }
]
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "CodeDeliveryDetailsList": [
    {
      "AttributeName": "email",
      "DeliveryMedium": "EMAIL",
      "Destination": "j***@e***"
    }
  ]
}
```

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](#)

UpdateUserPool

Updates the configuration of a user pool. To avoid setting parameters to Amazon Cognito defaults, construct this API request to pass the existing configuration of your user pool, modified to include the changes that you want to make.

Important

With the exception of `UserPoolTier`, if you don't provide a value for an attribute, Amazon Cognito sets it to its default value.

You can get a list of the current user pool settings using [DescribeUserPool](#).

Note

This action might generate an SMS text message. Starting June 1, 2021, US telecom carriers require you to register an origination phone number before you can send SMS messages to US phone numbers. If you use SMS text messages in Amazon Cognito, you must register a phone number with [Amazon Pinpoint](#). Amazon Cognito uses the registered number automatically. Otherwise, Amazon Cognito users who must receive SMS messages might not be able to sign up, activate their accounts, or sign in.

If you have never used SMS text messages with Amazon Cognito or any other AWS service, Amazon Simple Notification Service might place your account in the SMS sandbox. In [sandbox mode](#), you can send messages only to verified phone numbers. After you test your app while in the sandbox environment, you can move out of the sandbox and into production. For more information, see [SMS message settings for Amazon Cognito user pools](#) in the *Amazon Cognito Developer Guide*.

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
  "AccountRecoverySetting": {
    "RecoveryMechanisms": [
      {
        "Name": "string",
        "Priority": number
      }
    ]
  },
  "AdminCreateUserConfig": {
    "AllowAdminCreateUserOnly": boolean,
    "InviteMessageTemplate": {
      "EmailMessage": "string",
      "EmailSubject": "string",
      "SMSMessage": "string"
    },
    "UnusedAccountValidityDays": number
  },
  "AutoVerifiedAttributes": [ "string" ],
  "DeletionProtection": "string",
  "DeviceConfiguration": {
    "ChallengeRequiredOnNewDevice": boolean,
    "DeviceOnlyRememberedOnUserPrompt": boolean
  },
  "EmailConfiguration": {
    "ConfigurationSet": "string",
    "EmailSendingAccount": "string",
    "From": "string",
    "ReplyToEmailAddress": "string",
    "SourceArn": "string"
  },
  "EmailVerificationMessage": "string",
  "EmailVerificationSubject": "string",
```



```

    "LambdaConfig": {
      "CreateAuthChallenge": "string",
      "CustomEmailSender": {
        "LambdaArn": "string",
        "LambdaVersion": "string"
      },
      "CustomMessage": "string",
      "CustomSMSSEnder": {
        "LambdaArn": "string",
        "LambdaVersion": "string"
      },
      "DefineAuthChallenge": "string",
      "InboundFederation": {
        "LambdaArn": "string",
        "LambdaVersion": "string"
      },
      "KMSKeyID": "string",
      "PostAuthentication": "string",
      "PostConfirmation": "string",
      "PreAuthentication": "string",
      "PreSignUp": "string",
      "PreTokenGeneration": "string",
      "PreTokenGenerationConfig": {
        "LambdaArn": "string",
        "LambdaVersion": "string"
      },
      "UserMigration": "string",
      "VerifyAuthChallengeResponse": "string"
    },
    "MfaConfiguration": "string",
    "Policies": {
      "PasswordPolicy": {
        "MinimumLength": number,
        "PasswordHistorySize": number,
        "RequireLowercase": boolean,
        "RequireNumbers": boolean,
        "RequireSymbols": boolean,
        "RequireUppercase": boolean,
        "TemporaryPasswordValidityDays": number
      },
      "SignInPolicy": {
        "AllowedFirstAuthFactors": [ "string" ]
      }
    }
  },

```

```

"PoolName": "string",
"SmsAuthenticationMessage": "string",
"SmsConfiguration": {
  "ExternalId": "string",
  "SnsCallerArn": "string",
  "SnsRegion": "string"
},
"SmsVerificationMessage": "string",
"UserAttributeUpdateSettings": {
  "AttributesRequireVerificationBeforeUpdate": [ "string" ]
},
"UserPoolAddOns": {
  "AdvancedSecurityAdditionalFlows": {
    "CustomAuthMode": "string"
  },
  "AdvancedSecurityMode": "string"
},
"UserPoolId": "string",
"UserPoolTags": {
  "string" : "string"
},
"UserPoolTier": "string",
"VerificationMessageTemplate": {
  "DefaultEmailOption": "string",
  "EmailMessage": "string",
  "EmailMessageByLink": "string",
  "EmailSubject": "string",
  "EmailSubjectByLink": "string",
  "SmsMessage": "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.

[AccountRecoverySetting](#)

The available verified method a user can use to recover their password when they call `ForgotPassword`. You can use this setting to define a preferred method when a user has more than one method available. With this setting, SMS doesn't qualify for a valid password recovery

mechanism if the user also has SMS multi-factor authentication (MFA) activated. In the absence of this setting, Amazon Cognito uses the legacy behavior to determine the recovery method where SMS is preferred through email.

Type: [AccountRecoverySettingType](#) object

Required: No

[AdminCreateUserConfig](#)

The configuration for administrative creation of users. Includes the template for the invitation message for new users, the duration of temporary passwords, and permitting self-service sign-up.

Type: [AdminCreateUserConfigType](#) object

Required: No

[AutoVerifiedAttributes](#)

The attributes that you want your user pool to automatically verify. Possible values: **email**, **phone_number**. For more information see [Verifying contact information at sign-up](#).

Type: Array of strings

Valid Values: phone_number | email

Required: No

[DeletionProtection](#)

When active, DeletionProtection prevents accidental deletion of your user pool. Before you can delete a user pool that you have protected against deletion, you must deactivate this feature.

When you try to delete a protected user pool in a DeleteUserPool API request, Amazon Cognito returns an InvalidParameterException error. To delete a protected user pool, send a new DeleteUserPool request after you deactivate deletion protection in an UpdateUserPool API request.

Type: String

Valid Values: ACTIVE | INACTIVE

Required: No

DeviceConfiguration

The device-remembering configuration for a user pool. Device remembering or device tracking is a "Remember me on this device" option for user pools that perform authentication with the device key of a trusted device in the back end, instead of a user-provided MFA code. For more information about device authentication, see [Working with user devices in your user pool](#). A null value indicates that you have deactivated device remembering in your user pool.

Note

When you provide a value for any DeviceConfiguration field, you activate the Amazon Cognito device-remembering feature. For more information, see [Working with devices](#).

Type: [DeviceConfigurationType](#) object

Required: No

EmailConfiguration

The email configuration of your user pool. The email configuration type sets your preferred sending method, AWS Region, and sender for email invitation and verification messages from your user pool.

Type: [EmailConfigurationType](#) object

Required: No

EmailVerificationMessage

This parameter is no longer used. See [VerificationMessageTemplateType](#).

This parameter is no longer used.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 20000.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s*]*\{####\}`
`[\p{L}\p{M}\p{S}\p{N}\p{P}\s*]*`

Required: No

EmailVerificationSubject

This parameter is no longer used. See [VerificationMessageTemplateType](#).

This parameter is no longer used.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 140.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s]+`

Required: No

LambdaConfig

A collection of user pool Lambda triggers. Amazon Cognito invokes triggers at several possible stages of authentication operations. Triggers can modify the outcome of the operations that invoked them.

Type: [LambdaConfigType](#) object

Required: No

MfaConfiguration

Sets multi-factor authentication (MFA) to be on, off, or optional. When ON, all users must set up MFA before they can sign in. When OPTIONAL, your application must make a client-side determination of whether a user wants to register an MFA device. For user pools with adaptive authentication with threat protection, choose OPTIONAL.

When MfaConfiguration is OPTIONAL, managed login doesn't automatically prompt users to set up MFA. Amazon Cognito generates MFA prompts in API responses and in managed login for users who have chosen and configured a preferred MFA factor.

Type: String

Valid Values: OFF | ON | OPTIONAL

Required: No

Policies

The password policy and sign-in policy in the user pool. The password policy sets options like password complexity requirements and password history. The sign-in policy sets the options available to applications in [choice-based authentication](#).

Type: [UserPoolPolicyType](#) object

Required: No

[PoolName](#)

The updated name of your user pool.

Type: String

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

Pattern: `[\w\s+=, .@- ]+`

Required: No

[SmsAuthenticationMessage](#)

The contents of the SMS message that your user pool sends to users in SMS authentication.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 140.

Pattern: `.*\{####\}.*`

Required: No

[SmsConfiguration](#)

The SMS configuration with the settings for your Amazon Cognito user pool to send SMS message with Amazon Simple Notification Service. To send SMS messages with Amazon SNS in the AWS Region that you want, the Amazon Cognito user pool uses an AWS Identity and Access Management (IAM) role in your AWS account. For more information see [SMS message settings](#).

Type: [SmsConfigurationType](#) object

Required: No

[SmsVerificationMessage](#)

This parameter is no longer used. See [VerificationMessageTemplateType](#).

This parameter is no longer used.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 140.

Pattern: `.*\{####\}.*`

Required: No

UserAttributeUpdateSettings

The settings for updates to user attributes. These settings include the property `AttributesRequireVerificationBeforeUpdate`, a user-pool setting that tells Amazon Cognito how to handle changes to the value of your users' email address and phone number attributes. For more information, see [Verifying updates to email addresses and phone numbers](#).

Type: [UserAttributeUpdateSettingsType](#) object

Required: No

UserPoolAddOns

Contains settings for activation of threat protection, including the operating mode and additional authentication types. To log user security information but take no action, set to `AUDIT`. To configure automatic security responses to potentially unwanted traffic to your user pool, set to `ENFORCED`.

For more information, see [Adding advanced security to a user pool](#). To activate this setting, your user pool must be on the [Plus tier](#).

Type: [UserPoolAddOnsType](#) object

Required: No

UserPoolId

The ID of the user pool you want to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

UserPoolTags

The tag keys and values to assign to the user pool. A tag is a label that you can use to categorize and manage user pools in different ways, such as by purpose, owner, environment, or other criteria.

Type: String to string map

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

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

Required: No

UserPoolTier

The user pool [feature plan](#), or tier. This parameter determines the eligibility of the user pool for features like managed login, access-token customization, and threat protection. Defaults to ESSENTIALS.

Type: String

Valid Values: LITE | ESSENTIALS | PLUS

Required: No

VerificationMessageTemplate

The template for the verification message that your user pool delivers to users who set an email address or phone number attribute.

Set the email message type that corresponds to your `DefaultEmailOption` selection. For `CONFIRM_WITH_LINK`, specify an `EmailMessageByLink` and leave `EmailMessage` blank. For `CONFIRM_WITH_CODE`, specify an `EmailMessage` and leave `EmailMessageByLink` blank. When you supply both parameters with either choice, Amazon Cognito returns an error.

Type: [VerificationMessageTemplateType](#) 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](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

FeatureUnavailableInTierException

This exception is thrown when a feature you attempted to configure isn't available in your current feature plan.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidEmailRoleAccessPolicyException

This exception is thrown when Amazon Cognito isn't allowed to use your email identity. HTTP status code: 400.

message

The message returned when you have an unverified email address or the identity policy isn't set on an email address that Amazon Cognito can access.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidSmsRoleAccessPolicyException

This exception is returned when the role provided for SMS configuration doesn't have permission to publish using Amazon SNS.

message

The message returned when the invalid SMS role access policy exception is thrown.

HTTP Status Code: 400

InvalidSmsRoleTrustRelationshipException

This exception is thrown when the trust relationship is not valid for the role provided for SMS configuration. This can happen if you don't trust `cognito-idp.amazonaws.com` or the external ID provided in the role does not match what is provided in the SMS configuration for the user pool.

message

The message returned when the role trust relationship for the SMS message is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TierChangeNotAllowedException

This exception is thrown when you've attempted to change your feature plan but the operation isn't permitted.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserImportInProgressException

This exception is thrown when you're trying to modify a user pool while a user import job is in progress for that pool.

message

The message returned when the user pool has an import job running.

HTTP Status Code: 400

UserPoolTaggingException

This exception is thrown when a user pool tag can't be set or updated.

HTTP Status Code: 400

Examples

Example

The following `UpdateUserPool` request updates some common features of the target user pool.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.ca-central-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.UpdateUserPool
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
```

```
{
  "AccountRecoverySetting": {
    "RecoveryMechanisms": [
      {
        "Name": "verified_email",
        "Priority": 1
      },
      {
        "Name": "verified_phone_number",
        "Priority": 2
      }
    ]
  },
  "AdminCreateUserConfig": {
    "AllowAdminCreateUserOnly": false,
    "UnusedAccountValidityDays": 7
  },
  "AliasAttributes": [
    "email",
    "phone_number",
    "preferred_username"
  ],
  "Arn": "arn:aws:cognito-idp:ca-central-1:123456789012:userpool/ca-
central-1_EXAMPLE",
  "AutoVerifiedAttributes": [
    "email"
  ],
  "DeletionProtection": "ACTIVE",
  "Domain": "cognitoexample",
  "EmailConfiguration": {
    "ConfigurationSet": "my-sesconfigset",
```

```
    "EmailSendingAccount": "DEVELOPER",
    "SourceArn": "arn:aws:ses:us-east-1:123456789012:identity/admin@example.com"
  },
  "LambdaConfig": {
    "PreSignUp": "arn:aws:lambda:ca-central-1:123456789012:function:my-function"
  },
  "MfaConfiguration": "OPTIONAL",
  "Name": "my-test-user-pool",
  "Policies": {
    "PasswordPolicy": {
      "MinimumLength": 8,
      "RequireLowercase": true,
      "RequireNumbers": true,
      "RequireSymbols": true,
      "RequireUppercase": true,
      "TemporaryPasswordValidityDays": 7
    },
    "SignInPolicy": {
      "AllowedFirstAuthFactors": [
        "PASSWORD",
        "EMAIL_OTP",
        "WEB_AUTHN"
      ]
    }
  },
  "SmsConfiguration": {
    "ExternalId": "ALPHA-BRAVO",
    "SnsCallerArn": "arn:aws:iam::123456789012:role/My-SMS-Role",
    "SnsRegion": "us-east-1"
  },
  "UserAttributeUpdateSettings": {
    "AttributesRequireVerificationBeforeUpdate": [
      "email"
    ]
  },
  "UsernameConfiguration": {
    "CaseSensitive": false
  },
  "UserPoolAddOns": {
    "AdvancedSecurityAdditionalFlows": {
    },
    "AdvancedSecurityMode": "OFF"
  },
  "UserPoolId": "ca-central-1_EXAMPLE",
```

```
{
  "UserPoolTags": {
  },
  "UserPoolTier": "PLUS",
  "VerificationMessageTemplate": {
    "DefaultEmailOption": "CONFIRM_WITH_CODE"
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
```

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](#)

UpdateUserPoolClient

Given a user pool app client ID, updates the configuration. To avoid setting parameters to Amazon Cognito defaults, construct this API request to pass the existing configuration of your app client, modified to include the changes that you want to make.

Important

If you don't provide a value for an attribute, Amazon Cognito sets it to its default value.

You can get a list of the current app client settings with [DescribeUserPoolClient](#).

Unlike app clients created in the console, Amazon Cognito doesn't automatically assign a branding style to app clients that you configure with this API operation. Managed login and classic hosted UI pages aren't available for your client until after you apply a branding style.

Apply a branding style with the [CreateManagedLoginBranding](#) operation. For more information, see [Managed login branding](#).

You can also use this operation to enable token revocation for user pool clients. For more information about revoking tokens, see [RevokeToken](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
```

```

"AccessTokenValidity": number,
"AllowedOAuthFlows": [ "string" ],
"AllowedOAuthFlowsUserPoolClient": boolean,
"AllowedOAuthScopes": [ "string" ],
"AnalyticsConfiguration": {
  "ApplicationArn": "string",
  "ApplicationId": "string",
  "ExternalId": "string",
  "RoleArn": "string",
  "UserDataShared": boolean
},
"AuthSessionValidity": number,
"CallbackURLs": [ "string" ],
"ClientId": "string",
"ClientName": "string",
"DefaultRedirectURI": "string",
"EnablePropagateAdditionalUserContextData": boolean,
"EnableTokenRevocation": boolean,
"ExplicitAuthFlows": [ "string" ],
"IdTokenValidity": number,
"LogoutURLs": [ "string" ],
"PreventUserExistenceErrors": "string",
"ReadAttributes": [ "string" ],
"RefreshTokenRotation": {
  "Feature": "string",
  "RetryGracePeriodSeconds": number
},
"RefreshTokenValidity": number,
"SupportedIdentityProviders": [ "string" ],
"TokenValidityUnits": {
  "AccessToken": "string",
  "IdToken": "string",
  "RefreshToken": "string"
},
"UserPoolId": "string",
"WriteAttributes": [ "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.

AccessTokenValidity

The access token time limit. After this limit expires, your user can't use their access token. To specify the time unit for `AccessTokenValidity` as seconds, minutes, hours, or days, set a `TokenValidityUnits` value in your API request.

For example, when you set `AccessTokenValidity` to 10 and `TokenValidityUnits` to hours, your user can authorize access with their access token for 10 hours.

The default time unit for `AccessTokenValidity` in an API request is hours. *Valid range* is displayed below in seconds.

If you don't specify otherwise in the configuration of your app client, your access tokens are valid for one hour.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 86400.

Required: No

AllowedOAuthFlows

The OAuth grant types that you want your app client to generate. To create an app client that generates client credentials grants, you must add `client_credentials` as the only allowed OAuth flow.

`code`

Use a code grant flow, which provides an authorization code as the response. This code can be exchanged for access tokens with the `/oauth2/token` endpoint.

`implicit`

Issue the access token (and, optionally, ID token, based on scopes) directly to your user.

`client_credentials`

Issue the access token from the `/oauth2/token` endpoint directly to a non-person user using a combination of the client ID and client secret.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 3 items.

Valid Values: `code` | `implicit` | `client_credentials`

Required: No

[AllowedOAuthFlowsUserPoolClient](#)

Set to `true` to use OAuth 2.0 authorization server features in your app client.

This parameter must have a value of `true` before you can configure the following features in your app client.

- `CallbackURLs`: Callback URLs.
- `LogoutURLs`: Sign-out redirect URLs.
- `AllowedOAuthScopes`: OAuth 2.0 scopes.
- `AllowedOAuthFlows`: Support for authorization code, implicit, and client credentials OAuth 2.0 grants.

To use authorization server features, configure one of these features in the Amazon Cognito console or set `AllowedOAuthFlowsUserPoolClient` to `true` in a `CreateUserPoolClient` or `UpdateUserPoolClient` API request. If you don't set a value for `AllowedOAuthFlowsUserPoolClient` in a request with the AWS CLI or SDKs, it defaults to `false`. When `false`, only SDK-based API sign-in is permitted.

Type: Boolean

Required: No

[AllowedOAuthScopes](#)

The OAuth, OpenID Connect (OIDC), and custom scopes that you want to permit your app client to authorize access with. Scopes govern access control to user pool self-service API operations, user data from the `userInfo` endpoint, and third-party APIs. Scope values include `phone`, `email`, `openid`, and `profile`. The `aws.cognito.signin.user.admin` scope authorizes user self-service operations. Custom scopes with resource servers authorize access to external APIs.

Type: Array of strings

Array Members: Maximum number of 50 items.

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

Pattern: `[\x21\x23-\x5B\x5D-\x7E]+`

Required: No

[AnalyticsConfiguration](#)

The user pool analytics configuration for collecting metrics and sending them to your Amazon Pinpoint campaign.

In AWS Regions where Amazon Pinpoint isn't available, user pools might not have access to analytics or might be configurable with campaigns in the US East (N. Virginia) Region. For more information, see [Using Amazon Pinpoint analytics](#).

Type: [AnalyticsConfigurationType](#) object

Required: No

[AuthSessionValidity](#)

Amazon Cognito creates a session token for each API request in an authentication flow. `AuthSessionValidity` is the duration, in minutes, of that session token. Your user pool native user must respond to each authentication challenge before the session expires.

Type: Integer

Valid Range: Minimum value of 3. Maximum value of 15.

Required: No

[CallbackURLs](#)

A list of allowed redirect, or callback, URLs for managed login authentication. These URLs are the paths where you want to send your users' browsers after they complete authentication with managed login or a third-party IdP. Typically, callback URLs are the home of an application that uses OAuth or OIDC libraries to process authentication outcomes.

A redirect URI must meet the following requirements:

- Be an absolute URI.
- Be registered with the authorization server. Amazon Cognito doesn't accept authorization requests with `redirect_uri` values that aren't in the list of `CallbackURLs` that you provide in this parameter.
- Not include a fragment component.

See [OAuth 2.0 - Redirection Endpoint](#).

Amazon Cognito requires HTTPS over HTTP except for `http://localhost` for testing purposes only.

App callback URLs such as `myapp://example` are also supported.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: No

ClientId

The ID of the app client that you want to update.

Type: String

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

Pattern: `[\w+]+`

Required: Yes

ClientName

A friendly name for the app client.

Type: String

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

Pattern: `[\w\s+=, .@-]+`

Required: No

DefaultRedirectURI

The default redirect URI. In app clients with one assigned IdP, replaces `redirect_uri` in authentication requests. Must be in the `CallbackURLs` list.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: No

EnablePropagateAdditionalUserContextData

When `true`, your application can include additional `UserContextData` in authentication requests. This data includes the IP address, and contributes to analysis by threat protection features. For more information about propagation of user context data, see [Adding session data to API requests](#). If you don't include this parameter, you can't send the source IP address to Amazon Cognito threat protection features. You can only activate `EnablePropagateAdditionalUserContextData` in an app client that has a client secret.

Type: Boolean

Required: No

EnableTokenRevocation

Activates or deactivates [token revocation](#) in the target app client.

Revoke tokens with [RevokeToken](#).

Type: Boolean

Required: No

ExplicitAuthFlows

The [authentication flows](#) that you want your user pool client to support. For each app client in your user pool, you can sign in your users with any combination of one or more flows, including with a user name and Secure Remote Password (SRP), a user name and password, or a custom authentication process that you define with Lambda functions.

Note

If you don't specify a value for `ExplicitAuthFlows`, your app client supports `ALLOW_REFRESH_TOKEN_AUTH`, `ALLOW_USER_SRP_AUTH`, and `ALLOW_CUSTOM_AUTH`.

The values for authentication flow options include the following.

- **ALLOW_USER_AUTH**: Enable selection-based sign-in with **USER_AUTH**. This setting covers username-password, secure remote password (SRP), passwordless, and passkey authentication. This authentication flow can do username-password and SRP authentication without other **ExplicitAuthFlows** permitting them. For example users can complete an SRP challenge through **USER_AUTH** without the flow **USER_SRP_AUTH** being active for the app client. This flow doesn't include **CUSTOM_AUTH**.

To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

- **ALLOW_ADMIN_USER_PASSWORD_AUTH**: Enable admin based user password authentication flow **ADMIN_USER_PASSWORD_AUTH**. This setting replaces the **ADMIN_NO_SRP_AUTH** setting. With this authentication flow, your app passes a user name and password to Amazon Cognito in the request, instead of using the Secure Remote Password (SRP) protocol to securely transmit the password.
- **ALLOW_CUSTOM_AUTH**: Enable Lambda trigger based authentication.
- **ALLOW_USER_PASSWORD_AUTH**: Enable user password-based authentication. In this flow, Amazon Cognito receives the password in the request instead of using the SRP protocol to verify passwords.
- **ALLOW_USER_SRP_AUTH**: Enable SRP-based authentication.
- **ALLOW_REFRESH_TOKEN_AUTH**: Enable authflow to refresh tokens.

In some environments, you will see the values **ADMIN_NO_SRP_AUTH**, **CUSTOM_AUTH_FLOW_ONLY**, or **USER_PASSWORD_AUTH**. You can't assign these legacy **ExplicitAuthFlows** values to user pool clients at the same time as values that begin with **ALLOW_**, like **ALLOW_USER_SRP_AUTH**.

Type: Array of strings

Valid Values: **ADMIN_NO_SRP_AUTH** | **CUSTOM_AUTH_FLOW_ONLY** | **USER_PASSWORD_AUTH** | **ALLOW_ADMIN_USER_PASSWORD_AUTH** | **ALLOW_CUSTOM_AUTH** | **ALLOW_USER_PASSWORD_AUTH** | **ALLOW_USER_SRP_AUTH** | **ALLOW_REFRESH_TOKEN_AUTH** | **ALLOW_USER_AUTH**

Required: No

[IdTokenValidity](#)

The ID token time limit. After this limit expires, your user can't use their ID token. To specify the time unit for **IdTokenValidity** as seconds, minutes, hours, or days, set a **TokenValidityUnits** value in your API request.

For example, when you set `IdTokenValidity` as 10 and `TokenValidityUnits` as hours, your user can authenticate their session with their ID token for 10 hours.

The default time unit for `IdTokenValidity` in an API request is hours. *Valid range* is displayed below in seconds.

If you don't specify otherwise in the configuration of your app client, your ID tokens are valid for one hour.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 86400.

Required: No

LogoutURLs

A list of allowed logout URLs for managed login authentication. When you pass `logout_uri` and `client_id` parameters to `/logout`, Amazon Cognito signs out your user and redirects them to the logout URL. This parameter describes the URLs that you want to be the permitted targets of `logout_uri`. A typical use of these URLs is when a user selects "Sign out" and you redirect them to your public homepage. For more information, see [Logout endpoint](#).

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: No

PreventUserExistenceErrors

When `ENABLED`, suppresses messages that might indicate a valid user exists when someone attempts sign-in. This parameter sets your preference for the errors and responses that you want Amazon Cognito APIs to return during authentication, account confirmation, and password recovery when the user doesn't exist in the user pool. When set to `ENABLED` and the user doesn't exist, authentication returns an error indicating either the username or password was incorrect. Account confirmation and password recovery return a response indicating a code was sent to a simulated destination. When set to `LEGACY`, those APIs return a `UserNotFoundException` exception if the user doesn't exist in the user pool.

Defaults to LEGACY.

This setting affects the behavior of the following API operations.

- [AdminInitiateAuth](#)
- [AdminRespondToAuthChallenge](#)
- [InitiateAuth](#)
- [RespondToAuthChallenge](#)
- [ForgotPassword](#)
- [ConfirmForgotPassword](#)
- [ConfirmSignUp](#)
- [ResendConfirmationCode](#)

Type: String

Valid Values: LEGACY | ENABLED

Required: No

ReadAttributes

The list of user attributes that you want your app client to have read access to. After your user authenticates in your app, their access token authorizes them to read their own attribute value for any attribute in this list.

An example of this kind of activity is when your user selects a link to view their profile information. Your app makes a [GetUser](#) API request to retrieve and display your user's profile data.

When you don't specify the `ReadAttributes` for your app client, your app can read the values of `email_verified`, `phone_number_verified`, and the standard attributes of your user pool. When your user pool app client has read access to these default attributes, `ReadAttributes` doesn't return any information. Amazon Cognito only populates `ReadAttributes` in the API response if you have specified your own custom set of read attributes.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

RefreshTokenRotation

The configuration of your app client for refresh token rotation. When enabled, your app client issues new ID, access, and refresh tokens when users renew their sessions with refresh tokens. When disabled, token refresh issues only ID and access tokens.

Refresh token rotation must be completed with [GetTokensFromRefreshToken](#). With refresh token rotation disabled, you can complete token refresh with `GetTokensFromRefreshToken` and with `REFRESH_TOKEN_AUTH` in [InitiateAuth:AuthFlow](#) and [AdminInitiateAuth:AuthFlow](#).

Type: [RefreshTokenRotationType](#) object

Required: No

RefreshTokenValidity

The refresh token time limit. After this limit expires, your user can't use their refresh token. To specify the time unit for `RefreshTokenValidity` as seconds, minutes, hours, or days, set a `TokenValidityUnits` value in your API request.

For example, when you set `RefreshTokenValidity` as 10 and `TokenValidityUnits` as days, your user can refresh their session and retrieve new access and ID tokens for 10 days.

The default time unit for `RefreshTokenValidity` in an API request is days. You can't set `RefreshTokenValidity` to 0. If you do, Amazon Cognito overrides the value with the default value of 30 days. *Valid range* is displayed below in seconds.

If you don't specify otherwise in the configuration of your app client, your refresh tokens are valid for 30 days.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 315360000.

Required: No

SupportedIdentityProviders

A list of provider names for the identity providers (IdPs) that are supported on this client. The following are supported: COGNITO, Facebook, Google, SignInWithApple, and

LoginWithAmazon. You can also specify the names that you configured for the SAML and OIDC IdPs in your user pool, for example MySAMLIdP or MyOIDCIdP.

This parameter sets the IdPs that [managed login](#) will display on the login page for your app client. The removal of COGNITO from this list doesn't prevent authentication operations for local users with the user pools API in an AWS SDK. The only way to prevent SDK-based authentication is to block access with a [AWS WAF rule](#).

Type: Array of strings

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\p{Z}]+`

Required: No

[TokenValidityUnits](#)

The units that validity times are represented in. The default unit for refresh tokens is days, and the default for ID and access tokens are hours.

Type: [TokenValidityUnitsType](#) object

Required: No

[UserPoolId](#)

The ID of the user pool where you want to update the app client.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: Yes

[WriteAttributes](#)

The list of user attributes that you want your app client to have write access to. After your user authenticates in your app, their access token authorizes them to set or modify their own attribute value for any attribute in this list.

An example of this kind of activity is when you present your user with a form to update their profile information and they change their last name. Your app then makes an [UpdateUserAttributes](#) API request and sets `family_name` to the new value.

When you don't specify the `WriteAttributes` for your app client, your app can write the values of the Standard attributes of your user pool. When your user pool has write access to these default attributes, `WriteAttributes` doesn't return any information. Amazon Cognito only populates `WriteAttributes` in the API response if you have specified your own custom set of write attributes.

If your app client allows users to sign in through an IdP, this array must include all attributes that you have mapped to IdP attributes. Amazon Cognito updates mapped attributes when users sign in to your application through an IdP. If your app client does not have write access to a mapped attribute, Amazon Cognito throws an error when it tries to update the attribute. For more information, see [Specifying IdP Attribute Mappings for Your user pool](#).

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

Response Syntax

```
{
  "UserPoolClient": {
    "AccessTokenValidity": number,
    "AllowedOAuthFlows": [ "string" ],
    "AllowedOAuthFlowsUserPoolClient": boolean,
    "AllowedOAuthScopes": [ "string" ],
    "AnalyticsConfiguration": {
      "ApplicationArn": "string",
      "ApplicationId": "string",
      "ExternalId": "string",
      "RoleArn": "string",
      "UserDataShared": boolean
    },
    "AuthSessionValidity": number,
    "CallbackURLs": [ "string" ],
    "ClientId": "string",
    "ClientName": "string",
```

```
{
  "ClientSecret": "string",
  "CreationDate": number,
  "DefaultRedirectURI": "string",
  "EnablePropagateAdditionalUserContextData": boolean,
  "EnableTokenRevocation": boolean,
  "ExplicitAuthFlows": [ "string" ],
  "IdTokenValidity": number,
  "LastModifiedDate": number,
  "LogoutURLs": [ "string" ],
  "PreventUserExistenceErrors": "string",
  "ReadAttributes": [ "string" ],
  "RefreshTokenRotation": {
    "Feature": "string",
    "RetryGracePeriodSeconds": number
  },
  "RefreshTokenValidity": number,
  "SupportedIdentityProviders": [ "string" ],
  "TokenValidityUnits": {
    "AccessToken": "string",
    "IdToken": "string",
    "RefreshToken": "string"
  },
  "UserPoolId": "string",
  "WriteAttributes": [ "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.

UserPoolClient

The updated details of your app client.

Type: [UserPoolClientType](#) object

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

FeatureUnavailableInTierException

This exception is thrown when a feature you attempted to configure isn't available in your current feature plan.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidOAuthFlowException

This exception is thrown when the specified OAuth flow is not valid.

HTTP Status Code: 400

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

ScopeDoesNotExistException

This exception is thrown when the specified scope doesn't exist.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request updates an app client.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.UpdateUserPoolClient
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
    "UserPoolId": "us-west-2_EXAMPLE",
    "ClientName": "my-test-app",
    "ClientId": "1example23456789",
    "RefreshTokenValidity": 30,
    "AccessTokenValidity": 60,
    "IdTokenValidity": 60,
    "TokenValidityUnits": {
        "AccessToken": "minutes",
        "IdToken": "minutes",
        "RefreshToken": "days"
    },
    "ReadAttributes": [
        "address",
        "birthdate",
        "custom:state",
        "custom:accesstoken",
        "custom:idtoken",
        "email",
        "email_verified",
        "family_name",
        "gender",
        "locale",
        "middle_name",
        "name",
        "nickname",
        "phone_number",
        "phone_number_verified",
        "picture",
        "preferred_username",
        "profile",
        "updated_at",
        "website",
    ],
}
```

```
        "zoneinfo"
    ],
    "WriteAttributes": [
        "address",
        "birthdate",
        "custom:state",
        "custom:accesstoken",
        "custom:idtoken",
        "email",
        "family_name",
        "gender",
        "locale",
        "middle_name",
        "name",
        "nickname",
        "phone_number",
        "picture",
        "preferred_username",
        "profile",
        "updated_at",
        "website",
        "zoneinfo"
    ],
    "ExplicitAuthFlows": [
        "ALLOW_ADMIN_USER_PASSWORD_AUTH",
        "ALLOW_CUSTOM_AUTH",
        "ALLOW_REFRESH_TOKEN_AUTH",
        "ALLOW_USER_PASSWORD_AUTH",
        "ALLOW_USER_SRP_AUTH"
    ],
    "SupportedIdentityProviders": [
        "MYSSO",
        "COGNITO",
        "Google"
    ],
    "CallbackURLs": [
        "https://www.example.com",
        "https://app2.example.com"
    ],
    "LogoutURLs": [
        "https://auth.example.com/login?
client_id=1example23456789&response_type=code&redirect_uri=https%3A%2F
%2Fwww.example.com",
        "https://example.com/logout"
```



```
    ],
    "Allowed0AuthFlows": [
      "code",
      "implicit"
    ],
    "Allowed0AuthScopes": [
      "aws.cognito.signin.user.admin",
      "email",
      "openid",
      "phone",
      "profile"
    ],
    "Allowed0AuthFlowsUserPoolClient": true,
    "AnalyticsConfiguration": {
      "ApplicationArn": "arn:aws:mobiletargeting:us-
west-2:123456789012:apps/555666example",
      "UserDataShared": true
    },
    "PreventUserExistenceErrors": "LEGACY",
    "EnableTokenRevocation": true,
    "EnablePropagateAdditionalUserContextData": false,
    "AuthSessionValidity": 3
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "UserPoolClient": {
    "AccessTokenValidity": 60,
    "Allowed0AuthFlows": [
      "implicit",
      "code"
    ],
    "Allowed0AuthFlowsUserPoolClient": true,
    "Allowed0AuthScopes": [
      "aws.cognito.signin.user.admin",
      "phone",
```

```
        "openid",
        "profile",
        "email"
    ],
    "AnalyticsConfiguration": {
        "ApplicationArn": "arn:aws:mobiletargeting:us-
west-2:123456789012:apps/555666example",
        "RoleArn": "arn:aws:iam::123456789012:role/aws-service-role/cognito-
idp.amazonaws.com/AWSServiceRoleForAmazonCognitoIdp",
        "UserDataShared": true
    },
    "AuthSessionValidity": 3,
    "CallbackURLs": [
        "https://www.example.com",
        "https://app2.example.com"
    ],
    "ClientId": "1example23456789",
    "ClientName": "my-test-app",
    "CreationDate": 1603840085.621,
    "EnablePropagateAdditionalUserContextData": false,
    "EnableTokenRevocation": true,
    "ExplicitAuthFlows": [
        "ALLOW_CUSTOM_AUTH",
        "ALLOW_USER_PASSWORD_AUTH",
        "ALLOW_ADMIN_USER_PASSWORD_AUTH",
        "ALLOW_USER_SRP_AUTH",
        "ALLOW_REFRESH_TOKEN_AUTH"
    ],
    "IdTokenValidity": 60,
    "LastModifiedDate": 1736445292.513,
    "LogoutURLs": [
        "https://auth.example.com/login?
client_id=1example23456789&response_type=code&redirect_uri=https%3A%2F
%2Fwww.example.com",
        "https://example.com/logout"
    ],
    "PreventUserExistenceErrors": "LEGACY",
    "ReadAttributes": [
        "address",
        "birthdate",
        "custom:state",
        "custom:accesstoken",
        "custom:idtoken",
        "email",
```

```
        "email_verified",
        "family_name",
        "gender",
        "locale",
        "middle_name",
        "name",
        "nickname",
        "phone_number",
        "phone_number_verified",
        "picture",
        "preferred_username",
        "profile",
        "updated_at",
        "website",
        "zoneinfo"
    ],
    "RefreshTokenValidity": 30,
    "SupportedIdentityProviders": [
        "MYSSO",
        "COGNITO",
        "Google"
    ],
    "TokenValidityUnits": {
        "AccessToken": "minutes",
        "IdToken": "minutes",
        "RefreshToken": "days"
    },
    "UserPoolId": "us-west-2_EXAMPLE",
    "WriteAttributes": [
        "address",
        "birthdate",
        "custom:state",
        "custom:accesstoken",
        "custom:idtoken",
        "email",
        "family_name",
        "gender",
        "locale",
        "middle_name",
        "name",
        "nickname",
        "phone_number",
        "picture",
        "preferred_username",
```

```
        "profile",  
        "updated_at",  
        "website",  
        "zoneinfo"  
    ]  
}  
}
```

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](#)

UpdateUserPoolDomain

A user pool domain hosts managed login, an authorization server and web server for authentication in your application. This operation updates the branding version for user pool domains between 1 for hosted UI (classic) and 2 for managed login. It also updates the SSL certificate for user pool custom domains.

Changes to the domain branding version take up to one minute to take effect for a prefix domain and up to five minutes for a custom domain.

This operation doesn't change the name of your user pool domain. To change your domain, delete it with `DeleteUserPoolDomain` and create a new domain with `CreateUserPoolDomain`.

You can pass the ARN of a new AWS Certificate Manager certificate in this request. Typically, ACM certificates automatically renew and you user pool can continue to use the same ARN. But if you generate a new certificate for your custom domain name, replace the original configuration with the new ARN in this request.

ACM certificates for custom domains must be in the US East (N. Virginia) AWS Region. After you submit your request, Amazon Cognito requires up to 1 hour to distribute your new certificate to your custom domain.

For more information about adding a custom domain to your user pool, see [Configuring a user pool domain](#).

Note

Amazon Cognito evaluates AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you must use IAM credentials to authorize requests, and you must grant yourself the corresponding IAM permission in a policy.

Learn more

- [Signing AWS API Requests](#)
- [Using the Amazon Cognito user pools API and user pool endpoints](#)

Request Syntax

```
{
```

```
"CustomDomainConfig": {  
  "CertificateArn": "string",  
},  
"Domain": "string",  
"ManagedLoginVersion": number,  
"UserPoolId": "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.

[CustomDomainConfig](#)

The configuration for a custom domain that hosts managed login for your application. In an `UpdateUserPoolDomain` request, this parameter specifies an SSL certificate for the managed login hosted webserver. The certificate must be an ACM ARN in `us-east-1`.

When you create a custom domain, the passkey RP ID defaults to the custom domain. If you had a prefix domain active, this will cause passkey integration for your prefix domain to stop working due to a mismatch in RP ID. To keep the prefix domain passkey integration working, you can explicitly set RP ID to the prefix domain.

Update the RP ID in a [SetUserPoolMfaConfig](#) request.

Type: [CustomDomainConfigType](#) object

Required: No

[Domain](#)

The name of the domain that you want to update. For custom domains, this is the fully-qualified domain name, for example `auth.example.com`. For prefix domains, this is the prefix alone, such as `myprefix`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 63.

Pattern: `^[a-z0-9](?:[a-z0-9\-\]{0,61}[a-z0-9])?$`

Required: Yes

ManagedLoginVersion

A version number that indicates the state of managed login for your domain. Version 1 is hosted UI (classic). Version 2 is the newer managed login with the branding editor. For more information, see [Managed login](#).

Type: Integer

Required: No

UserPoolId

The ID of the user pool that is associated with the domain you're updating.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: Yes

Response Syntax

```
{
  "CloudFrontDomain": "string",
  "ManagedLoginVersion": 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.

CloudFrontDomain

The fully-qualified domain name (FQDN) of the Amazon CloudFront distribution that hosts your managed login or classic hosted UI pages. Your domain-name authority must have an alias record that points requests for your custom domain to this FQDN. Amazon Cognito returns this

value if you set a custom domain with `CustomDomainConfig`. If you set an Amazon Cognito prefix domain, this operation returns a blank response.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 63.

Pattern: `^[a-z0-9](?:[a-z0-9\-\-]{0,61}[a-z0-9])?$`

ManagedLoginVersion

A version number that indicates the state of managed login for your domain. Version 1 is hosted UI (classic). Version 2 is the newer managed login with the branding editor. For more information, see [Managed login](#).

Type: Integer

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

ConcurrentModificationException

This exception is thrown if two or more modifications are happening concurrently.

message

The message provided when the concurrent exception is thrown.

HTTP Status Code: 400

FeatureUnavailableInTierException

This exception is thrown when a feature you attempted to configure isn't available in your current feature plan.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

Examples

Example

The following example request configures an ACM certificate and sets the managed login branding version to 2 for a custom domain.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.ca-central-1.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.UpdateUserPoolDomain
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "CustomDomainConfig": {
    "CertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Domain": "auth.example.com",
  "ManagedLoginVersion": 2,
  "UserPoolId": "ca-central-1_EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "CloudFrontDomain": "example.cloudfront.net",
  "ManagedLoginVersion": 2
}
```

```
}
```

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](#)

VerifySoftwareToken

Registers the current user's time-based one-time password (TOTP) authenticator with a code generated in their authenticator app from a private key that's supplied by your user pool. Marks the user's software token MFA status as "verified" if successful. The request takes an access token or a session string, but not both.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{
  "AccessToken": "string",
  "FriendlyDeviceName": "string",
  "Session": "string",
  "UserCode": "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.

AccessToken

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws:cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: No

FriendlyDeviceName

A friendly name for the device that's running the TOTP authenticator.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

Session

The session ID from an AssociateSoftwareToken request.

Type: String

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

Required: No

UserCode

A TOTP that the user generated in their configured authenticator app.

Type: String

Length Constraints: Fixed length of 6.

Pattern: [0-9] +

Required: Yes

Response Syntax

```
{  
  "Session": "string",  
  "Status": "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.

Session

This session ID satisfies an MFA_SETUP challenge. Supply the session ID in your challenge response.

Operations that can return an MFA_SETUP challenge include [InitiateAuth](#), [AdminInitiateAuth](#), [RespondToAuthChallenge](#), and [AdminRespondToAuthChallenge](#).

Type: String

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

Status

Amazon Cognito can accept or reject the code that you provide. This response parameter indicates the success of TOTP verification. Some reasons that this operation might return an error are clock skew on the user's device and excessive retries.

Type: String

Valid Values: SUCCESS | ERROR

Errors

For information about the errors that are common to all actions, see [Common Error Types](#).

CodeMismatchException

This exception is thrown if the provided code doesn't match what the server was expecting.

message

The message provided when the code mismatch exception is thrown.

HTTP Status Code: 400

EnableSoftwareTokenMFAException

This exception is thrown when there is a code mismatch and the service fails to configure the software token TOTP multi-factor authentication (MFA).

HTTP Status Code: 400

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

InvalidUserPoolConfigurationException

This exception is thrown when the user pool configuration is not valid.

message

The message returned when the user pool configuration is not valid.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

SoftwareTokenMFANotFoundException

This exception is thrown when the software token time-based one-time password (TOTP) multi-factor authentication (MFA) isn't activated for the user pool.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request activates TOTP MFA for the current user.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.VerifySoftwareToken
User-Agent: <UserAgentString>
```

```
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE",
  "FriendlyDeviceName": "MyAuthenticatorApp",
  "UserCode": "123456"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{
  "Status": "SUCCESS"
}
```

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](#)

VerifyUserAttribute

Submits a verification code for a signed-in user who has added or changed a value of an auto-verified attribute. When successful, the user's attribute becomes verified and the attribute `email_verified` or `phone_number_verified` becomes `true`.

If your user pool requires verification before Amazon Cognito updates the attribute value, this operation updates the affected attribute to its pending value.

See also [UserAttributeUpdateSettingsType](#).

Authorize this action with a signed-in user's access token. It must include the scope `aws.cognito.signin.user.admin`.

Note

Amazon Cognito doesn't evaluate AWS Identity and Access Management (IAM) policies in requests for this API operation. For this operation, you can't use IAM credentials to authorize requests, and you can't grant IAM permissions in policies. For more information about authorization models in Amazon Cognito, see [Using the Amazon Cognito user pools API and user pool endpoints](#).

Request Syntax

```
{
  "AccessToken": "string",
  "AttributeName": "string",
  "Code": "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.

AccessToken

A valid access token that Amazon Cognito issued to the currently signed-in user. Must include a scope claim for `aws:cognito.signin.user.admin`.

Type: String

Pattern: `[A-Za-z0-9-_.]+`

Required: Yes

AttributeName

The name of the attribute that you want to verify.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\t\n\r ]+`

Required: Yes

Code

The verification code that your user pool sent to the added or changed attribute, for example the user's email address.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[\S]+`

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](#).

AliasExistsException

This exception is thrown when a user tries to confirm the account with an email address or phone number that has already been supplied as an alias for a different user profile. This exception indicates that an account with this email address or phone already exists in a user pool that you've configured to use email address or phone number as a sign-in alias.

message

The message that Amazon Cognito sends to the user when the value of an alias attribute is already linked to another user profile.

HTTP Status Code: 400

CodeMismatchException

This exception is thrown if the provided code doesn't match what the server was expecting.

message

The message provided when the code mismatch exception is thrown.

HTTP Status Code: 400

ExpiredCodeException

This exception is thrown if a code has expired.

message

The message returned when the expired code exception is thrown.

HTTP Status Code: 400

ForbiddenException

This exception is thrown when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

message

The message returned when AWS WAF doesn't allow your request based on a web ACL that's associated with your user pool.

HTTP Status Code: 400

InternalErrorException

This exception is thrown when Amazon Cognito encounters an internal error.

message

The message returned when Amazon Cognito throws an internal error exception.

HTTP Status Code: 500

InvalidParameterException

This exception is thrown when the Amazon Cognito service encounters an invalid parameter.

message

The message returned when the Amazon Cognito service throws an invalid parameter exception.

reasonCode

The reason code of the exception.

HTTP Status Code: 400

LimitExceededException

This exception is thrown when a user exceeds the limit for a requested AWS resource.

message

The message returned when Amazon Cognito throws a limit exceeded exception.

HTTP Status Code: 400

NotAuthorizedException

This exception is thrown when a user isn't authorized.

message

The message returned when the Amazon Cognito service returns a not authorized exception.

HTTP Status Code: 400

PasswordResetRequiredException

This exception is thrown when a password reset is required.

message

The message returned when a password reset is required.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the Amazon Cognito service can't find the requested resource.

message

The message returned when the Amazon Cognito service returns a resource not found exception.

HTTP Status Code: 400

TooManyRequestsException

This exception is thrown when the user has made too many requests for a given operation.

message

The message returned when the Amazon Cognito service returns a too many requests exception.

HTTP Status Code: 400

UserNotConfirmedException

This exception is thrown when a user isn't confirmed successfully.

message

The message returned when a user isn't confirmed successfully.

HTTP Status Code: 400

UserNotFoundException

This exception is thrown when a user isn't found.

message

The message returned when a user isn't found.

HTTP Status Code: 400

Examples

Example

The following example request verifies the email attribute for the current user with a code that was sent in an email message to them.

Sample Request

```
POST HTTP/1.1
Host: cognito-idp.us-west-2.amazonaws.com
X-Amz-Date: 20230613T200059Z
Accept-Encoding: gzip, deflate, br
X-Amz-Target: AWSCognitoIdentityProviderService.VerifyUserAttribute
User-Agent: <UserAgentString>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
  Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "AccessToken": "eyJra456defEXAMPLE",
  "AttributeName": "email",
  "Code": "123456"
}
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2023 20:00:59 GMT
Content-Type: application/x-amz-json-1.0
Content-Length: <PayloadSizeBytes>
x-amzn-requestid: a1b2c3d4-e5f6-a1b2-c3d4-EXAMPLE11111
Connection: keep-alive
{}
```

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 Amazon Cognito Identity Provider 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:

- [AccountRecoverySettingType](#)
- [AccountTakeoverActionsType](#)
- [AccountTakeoverActionType](#)
- [AccountTakeoverRiskConfigurationType](#)
- [AdminCreateUserConfigType](#)
- [AdvancedSecurityAdditionalFlowsType](#)
- [AnalyticsConfigurationType](#)
- [AnalyticsMetadataType](#)
- [AssetType](#)
- [AttributeType](#)
- [AuthenticationResultType](#)
- [AuthEventType](#)
- [ChallengeResponseType](#)
- [ClientSecretDescriptorType](#)
- [ClientSecretListDescriptorType](#)
- [CloudWatchLogsConfigurationType](#)
- [CodeDeliveryDetailsType](#)
- [CompromisedCredentialsActionsType](#)
- [CompromisedCredentialsRiskConfigurationType](#)
- [ContextDataType](#)

- [CustomDomainConfigType](#)
- [CustomEmailLambdaVersionConfigType](#)
- [CustomSMSLambdaVersionConfigType](#)
- [DeviceConfigurationType](#)
- [DeviceSecretVerifierConfigType](#)
- [DeviceType](#)
- [DomainDescriptionType](#)
- [EmailConfigurationType](#)
- [EmailMfaConfigType](#)
- [EmailMfaSettingsType](#)
- [EventContextDataType](#)
- [EventFeedbackType](#)
- [EventRiskType](#)
- [FirehoseConfigurationType](#)
- [GroupType](#)
- [HTTPHeader](#)
- [IdentityProviderType](#)
- [InboundFederationLambdaType](#)
- [LambdaConfigType](#)
- [LogConfigurationType](#)
- [LogDeliveryConfigurationType](#)
- [ManagedLoginBrandingType](#)
- [MessageTemplateType](#)
- [MFAOptionType](#)
- [NewDeviceMetadataType](#)
- [NotifyConfigurationType](#)
- [NotifyEmailType](#)
- [NumberAttributeConstraintsType](#)
- [PasswordPolicyType](#)
- [PreTokenGenerationVersionConfigType](#)

- [ProviderDescription](#)
- [ProviderUserIdentifierType](#)
- [RecoveryOptionType](#)
- [RefreshTokenRotationType](#)
- [ResourceServerScopeType](#)
- [ResourceServerType](#)
- [RiskConfigurationType](#)
- [RiskExceptionConfigurationType](#)
- [S3ConfigurationType](#)
- [SchemaAttributeType](#)
- [SignInPolicyType](#)
- [SmsConfigurationType](#)
- [SmsMfaConfigType](#)
- [SMSMfaSettingsType](#)
- [SoftwareTokenMfaConfigType](#)
- [SoftwareTokenMfaSettingsType](#)
- [StringAttributeConstraintsType](#)
- [TermsDescriptionType](#)
- [TermsType](#)
- [TokenValidityUnitsType](#)
- [UICustomizationType](#)
- [UserAttributeUpdateSettingsType](#)
- [UserContextDataType](#)
- [UserImportJobType](#)
- [UsernameConfigurationType](#)
- [UserPoolAddOnsType](#)
- [UserPoolClientDescription](#)
- [UserPoolClientType](#)
- [UserPoolDescriptionType](#)
- [UserPoolPolicyType](#)

- [UserPoolType](#)
- [UserType](#)
- [VerificationMessageTemplateType](#)
- [WebAuthnConfigurationType](#)
- [WebAuthnCredentialDescription](#)
- [WebAuthnMfaSettingsType](#)

AccountRecoverySettingType

The settings for user message delivery in forgot-password operations. Contains preference for email or SMS message delivery of password reset codes, or for admin-only password reset.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

RecoveryMechanisms

The list of options and priorities for user message delivery in forgot-password operations. Sets or displays user pool preferences for email or SMS message priority, whether users should fall back to a second delivery method, and whether passwords should only be reset by administrators.

Type: Array of [RecoveryOptionType](#) objects

Array Members: Minimum number of 1 item. Maximum number of 2 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](#)

AccountTakeoverActionTypes

A list of account-takeover actions for each level of risk that Amazon Cognito might assess with threat protection features.

This data type is a request parameter of [SetRiskConfiguration](#) and a response parameter of [DescribeRiskConfiguration](#).

Contents

HighAction

The action that you assign to a high-risk assessment by threat protection.

Type: [AccountTakeoverActionType](#) object

Required: No

LowAction

The action that you assign to a low-risk assessment by threat protection.

Type: [AccountTakeoverActionType](#) object

Required: No

MediumAction

The action that you assign to a medium-risk assessment by threat protection.

Type: [AccountTakeoverActionType](#) 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](#)

AccountTakeoverActionType

The automated response to a risk level for adaptive authentication in full-function, or ENFORCED, mode. You can assign an action to each risk level that threat protection evaluates.

This data type is a request parameter of [SetRiskConfiguration](#) and a response parameter of [DescribeRiskConfiguration](#).

Contents

EventAction

The action to take for the attempted account takeover action for the associated risk level. Valid values are as follows:

- **BLOCK**: Block the request.
- **MFA_IF_CONFIGURED**: Present an MFA challenge if possible. MFA is possible if the user pool has active MFA methods that the user can set up. For example, if the user pool only supports SMS message MFA but the user doesn't have a phone number attribute, MFA setup isn't possible. If MFA setup isn't possible, allow the request.
- **MFA_REQUIRED**: Present an MFA challenge if possible. Block the request if a user hasn't set up MFA. To sign in with required MFA, users must have an email address or phone number attribute, or a registered TOTP factor.
- **NO_ACTION**: Take no action. Permit sign-in.

Type: String

Valid Values: BLOCK | MFA_IF_CONFIGURED | MFA_REQUIRED | NO_ACTION

Required: Yes

Notify

Determines whether Amazon Cognito sends a user a notification message when your user pools assesses a user's session at the associated risk level.

Type: Boolean

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](#)

AccountTakeoverRiskConfigurationType

The settings for automated responses and notification templates for adaptive authentication with threat protection features.

This data type is a request parameter of [SetRiskConfiguration](#) and a response parameter of [DescribeRiskConfiguration](#).

Contents

Actions

A list of account-takeover actions for each level of risk that Amazon Cognito might assess with threat protection.

Type: [AccountTakeoverActionsType](#) object

Required: Yes

NotifyConfiguration

The settings for composing and sending an email message when threat protection assesses a risk level with adaptive authentication. When you choose to notify users in `AccountTakeoverRiskConfiguration`, Amazon Cognito sends an email message using the method and template that you set with this data type.

Type: [NotifyConfigurationType](#) 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](#)

AdminCreateUserConfigType

The settings for administrator creation of users in a user pool. Contains settings for allowing user sign-up, customizing invitation messages to new users, and the amount of time before temporary passwords expire.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

AllowAdminCreateUserOnly

The setting for allowing self-service sign-up. When `true`, only administrators can create new user profiles. When `false`, users can register themselves and create a new user profile with the `SignUp` operation.

Type: Boolean

Required: No

InviteMessageTemplate

The template for the welcome message to new users. This template must include the `{#####}` temporary password placeholder if you are creating users with passwords. If your users don't have passwords, you can omit the placeholder.

See also [Customizing User Invitation Messages](#).

Type: [MessageTemplateType](#) object

Required: No

UnusedAccountValidityDays

This parameter is no longer in use.

Configure the duration of temporary passwords with the `TemporaryPasswordValidityDays` parameter of [PasswordPolicyType](#). For older user pools that have a `UnusedAccountValidityDays` configuration, that value is effective until you set a value for `TemporaryPasswordValidityDays`.

The password expiration limit in days for administrator-created users. When this time expires, the user can't sign in with their temporary password. To reset the account after that time limit, you must call `AdminCreateUser` again, specifying `RESEND` for the `MessageAction` parameter.

The default value for this parameter is 7.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 365.

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](#)

AdvancedSecurityAdditionalFlowsType

Threat protection configuration options for additional authentication types in your user pool, including custom authentication.

Contents

CustomAuthMode

The operating mode of threat protection in custom authentication with [Custom authentication challenge Lambda triggers](#).

Type: String

Valid Values: AUDIT | ENFORCED

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](#)

AnalyticsConfigurationType

The settings for Amazon Pinpoint analytics configuration. With an analytics configuration, your application can collect user-activity metrics for user notifications with a Amazon Pinpoint campaign.

Amazon Pinpoint isn't available in all AWS Regions. For a list of available Regions, see [Amazon Cognito and Amazon Pinpoint Region availability](#).

This data type is a request parameter of [CreateUserPoolClient](#) and [UpdateUserPoolClient](#), and a response parameter of [DescribeUserPoolClient](#).

Contents

ApplicationArn

The Amazon Resource Name (ARN) of an Amazon Pinpoint project that you want to connect to your user pool app client. Amazon Cognito publishes events to the Amazon Pinpoint project that ApplicationArn declares. You can also configure your application to pass an endpoint ID in the AnalyticsMetadata parameter of sign-in operations. The endpoint ID is information about the destination for push notifications

Type: String

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

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

Required: No

ApplicationId

Your Amazon Pinpoint project ID.

Type: String

Pattern: `^[0-9a-fA-F]+$`

Required: No

ExternalId

The [external ID](#) of the role that Amazon Cognito assumes to send analytics data to Amazon Pinpoint.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

RoleArn

The ARN of an AWS Identity and Access Management role that has the permissions required for Amazon Cognito to publish events to Amazon Pinpoint analytics.

Type: String

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

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

Required: No

UserDataShared

If `UserDataShared` is `true`, Amazon Cognito includes user data in the events that it publishes to Amazon Pinpoint analytics.

Type: Boolean

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](#)

AnalyticsMetadataType

Information that your application adds to authentication requests. Applies an endpoint ID to the analytics data that your user pool sends to Amazon Pinpoint.

An endpoint ID uniquely identifies a mobile device, email address or phone number that can receive messages from Amazon Pinpoint analytics. For more information about AWS Regions that can contain Amazon Pinpoint resources for use with Amazon Cognito user pools, see [Using Amazon Pinpoint analytics with Amazon Cognito user pools](#).

This data type is a request parameter of authentication operations like [InitiateAuth](#), [AdminInitiateAuth](#), [RespondToAuthChallenge](#), and [AdminRespondToAuthChallenge](#).

Contents

AnalyticsEndpointId

The endpoint ID. Information that you want to pass to Amazon Pinpoint about where to send notifications.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#)

AssetType

An image file from a managed login branding style in a user pool.

This data type is a request parameter of [CreateManagedLoginBranding](#) and [UpdateManagedLoginBranding](#), and a response parameter of [DescribeManagedLoginBranding](#).

Contents

Category

The category that the image corresponds to in your managed login configuration. Managed login has asset categories for different types of logos, backgrounds, and icons.

Type: String

Valid Values: FAVICON_ICO | FAVICON_SVG | EMAIL_GRAPHIC | SMS_GRAPHIC | AUTH_APP_GRAPHIC | PASSWORD_GRAPHIC | PASSKEY_GRAPHIC | PAGE_HEADER_LOGO | PAGE_HEADER_BACKGROUND | PAGE_FOOTER_LOGO | PAGE_FOOTER_BACKGROUND | PAGE_BACKGROUND | FORM_BACKGROUND | FORM_LOGO | IDP_BUTTON_ICON

Required: Yes

ColorMode

The display-mode target of the asset: light, dark, or browser-adaptive. For example, Amazon Cognito displays a dark-mode image only when the browser or application is in dark mode, but displays a browser-adaptive file in all contexts.

Type: String

Valid Values: LIGHT | DARK | DYNAMIC

Required: Yes

Extension

The file type of the image file.

Type: String

Valid Values: ICO | JPEG | PNG | SVG | WEBP

Required: Yes

Bytes

The image file, in Base64-encoded binary.

Type: Base64-encoded binary data object

Length Constraints: Maximum length of 1000000.

Required: No

ResourceId

The ID of the asset.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 40.

Pattern: `^[\\w\\- ]+$`

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](#)

AttributeType

The name and value of a user attribute.

This data type is a request parameter of [AdminUpdateUserAttributes](#) and [UpdateUserAttributes](#).

Contents

Name

The name of the attribute, for example email or custom:department.

In some older user pools, the regex pattern for acceptable values of this parameter is `[\p{L}\p{M}\p{S}\p{N}\p{P}]`+. Older pools will eventually be updated to use the new pattern. Affected user pools are those created before May 2024 in US East (N. Virginia), US East (Ohio), US West (N. California), US West (Oregon), Asia Pacific (Mumbai), Asia Pacific (Tokyo), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central), Europe (Frankfurt), Europe (Ireland), Europe (London), Europe (Paris), Europe (Stockholm), Middle East (Bahrain), and South America (São Paulo).

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\t\n\r ]`+

Required: Yes

Value

The value of the attribute.

Type: String

Length Constraints: Maximum length of 2048.

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](#)

AuthenticationResultType

The object that your application receives after authentication. Contains tokens and information for device authentication.

This data type is a response parameter of authentication operations like [InitiateAuth](#), [AdminInitiateAuth](#), [RespondToAuthChallenge](#), [AdminRespondToAuthChallenge](#), and [GetTokensFromRefreshToken](#). `GetTokensFromRefreshToken` doesn't return `NewDeviceMetadata`.

Contents

AccessToken

Your user's access token.

Type: String

Pattern: `[A-Za-z0-9-_=.]`+

Required: No

ExpiresIn

The expiration period of the authentication result in seconds.

Type: Integer

Required: No

IdToken

Your user's ID token.

Type: String

Pattern: `[A-Za-z0-9-_=.]`+

Required: No

NewDeviceMetadata

The new device metadata from an authentication result.

Type: [NewDeviceMetadataType](#) object

Required: No

RefreshToken

Your user's refresh token.

Type: String

Pattern: [A-Za-z0-9-_=.] +

Required: No

TokenType

The intended use of the token, for example Bearer.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#)

AuthEventType

One authentication event that Amazon Cognito logged in a user pool with threat protection active. Contains user and device metadata and a risk assessment from your user pool.

This data type is a response parameter of [AdminListUserAuthEvents](#).

Contents

ChallengeResponses

A list of the challenges that the user was requested to answer, for example Password, and the result, for example Success.

Type: Array of [ChallengeResponseType](#) objects

Required: No

CreationDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

EventContextData

The user context data captured at the time of an event request. This value provides additional information about the client from which event the request is received.

Type: [EventContextDataType](#) object

Required: No

EventFeedback

The UpdateAuthEventFeedback or AdminUpdateAuthEventFeedback feedback that you or your user provided in response to the event. A value of Valid indicates that you disagreed with the level of risk that your user pool assigned, and evaluated a session to be valid, or likely

safe. A value of `Invalid` indicates that you agreed with the user pool risk level and evaluated a session to be invalid, or likely malicious.

Type: [EventFeedbackType](#) object

Required: No

EventId

The event ID.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

EventResponse

The event response.

Type: String

Valid Values: `Pass` | `Fail` | `InProgress`

Required: No

EventRisk

The threat evaluation from your user pool about an event. Contains information about whether your user pool detected compromised credentials, whether the event triggered an automated response, and the level of risk.

Type: [EventRiskType](#) object

Required: No

EventType

The type of authentication event.

Type: String

Valid Values: `SignIn` | `SignUp` | `ForgotPassword` | `PasswordChange` | `ResendCode`

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](#)

ChallengeResponseType

The responses to the challenge that you received in the previous request. Each challenge has its own required response parameters. The following examples are partial JSON request bodies that highlight challenge-response parameters.

Important

You must provide a `SECRET_HASH` parameter in all challenge responses to an app client that has a client secret. Include a `DEVICE_KEY` for device authentication.

SELECT_CHALLENGE

```
"ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses": { "USERNAME": "[username]", "ANSWER": "[Challenge name]" }
```

Available challenges are `PASSWORD`, `PASSWORD_SRP`, `EMAIL_OTP`, `SMS_OTP`, and `WEB_AUTHN`.

Complete authentication in the `SELECT_CHALLENGE` response for `PASSWORD`, `PASSWORD_SRP`, and `WEB_AUTHN`:

- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses": { "ANSWER": "WEB_AUTHN", "USERNAME": "[username]", "CREDENTIAL": "[AuthenticationResponseJSON]" }

See [AuthenticationResponseJSON](#).

- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses": { "ANSWER": "PASSWORD", "USERNAME": "[username]", "PASSWORD": "[password]" }
- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses": { "ANSWER": "PASSWORD_SRP", "USERNAME": "[username]", "SRP_A": "[SRP_A]" }

For `SMS_OTP` and `EMAIL_OTP`, respond with the username and answer. Your user pool will send a code for the user to submit in the next challenge response.

- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses": { "ANSWER": "SMS_OTP", "USERNAME": "[username]" }
- "ChallengeName": "SELECT_CHALLENGE", "ChallengeResponses": { "ANSWER": "EMAIL_OTP", "USERNAME": "[username]" }

WEB_AUTHN

```
"ChallengeName": "WEB_AUTHN", "ChallengeResponses": { "USERNAME":  
"[username]", "CREDENTIAL": "[AuthenticationResponseJSON]" }
```

See [AuthenticationResponseJSON](#).

PASSWORD

```
"ChallengeName": "PASSWORD", "ChallengeResponses": { "USERNAME":  
"[username]", "PASSWORD": "[password]" }
```

PASSWORD_SRP

```
"ChallengeName": "PASSWORD_SRP", "ChallengeResponses": { "USERNAME":  
"[username]", "SRP_A": "[SRP_A]" }
```

SMS_OTP

```
"ChallengeName": "SMS_OTP", "ChallengeResponses": {"SMS_OTP_CODE":  
"[code]", "USERNAME": "[username]" }
```

EMAIL_OTP

```
"ChallengeName": "EMAIL_OTP", "ChallengeResponses": {"EMAIL_OTP_CODE":  
"[code]", "USERNAME": "[username]" }
```

SMS_MFA

```
"ChallengeName": "SMS_MFA", "ChallengeResponses": {"SMS_MFA_CODE":  
"[code]", "USERNAME": "[username]" }
```

PASSWORD_VERIFIER

This challenge response is part of the SRP flow. Amazon Cognito requires that your application respond to this challenge within a few seconds. When the response time exceeds this period, your user pool returns a `NotAuthorizedException` error.

```
"ChallengeName": "PASSWORD_VERIFIER", "ChallengeResponses":  
{ "PASSWORD_CLAIM_SIGNATURE": "[claim_signature]",  
  "PASSWORD_CLAIM_SECRET_BLOCK": "[secret_block]", "TIMESTAMP":  
  [timestamp], "USERNAME": "[username]" }
```

CUSTOM_CHALLENGE

```
"ChallengeName": "CUSTOM_CHALLENGE", "ChallengeResponses": {"USERNAME":  
"[username]", "ANSWER": "[challenge_answer]" }
```

NEW_PASSWORD_REQUIRED

```
"ChallengeName": "NEW_PASSWORD_REQUIRED", "ChallengeResponses":  
{ "NEW_PASSWORD": "[new_password]", "USERNAME": "[username]" }
```

To set any required attributes that `InitiateAuth` returned in an `requiredAttributes` parameter, add `"userAttributes.[attribute_name]": "[attribute_value]"`. This parameter can also set values for writable attributes that aren't required by your user pool.

Note

In a `NEW_PASSWORD_REQUIRED` challenge response, you can't modify a required attribute that already has a value. In `AdminRespondToAuthChallenge` or `RespondToAuthChallenge`, set a value for any keys that Amazon Cognito returned in the `requiredAttributes` parameter, then use the `AdminUpdateUserAttributes` or `UpdateUserAttributes` API operation to modify the value of any additional attributes.

SOFTWARE_TOKEN_MFA

```
"ChallengeName": "SOFTWARE_TOKEN_MFA", "ChallengeResponses":  
{ "USERNAME": "[username]", "SOFTWARE_TOKEN_MFA_CODE":  
  [authenticator_code] }
```

DEVICE_SRP_AUTH

```
"ChallengeName": "DEVICE_SRP_AUTH", "ChallengeResponses": { "USERNAME":  
  "[username]", "DEVICE_KEY": "[device_key]", "SRP_A": "[srp_a]" }
```

DEVICE_PASSWORD_VERIFIER

```
"ChallengeName": "DEVICE_PASSWORD_VERIFIER", "ChallengeResponses":  
{ "DEVICE_KEY": "[device_key]", "PASSWORD_CLAIM_SIGNATURE":  
  "[claim_signature]", "PASSWORD_CLAIM_SECRET_BLOCK": "[secret_block]",  
  "TIMESTAMP": [timestamp], "USERNAME": "[username]" }
```

MFA_SETUP

```
"ChallengeName": "MFA_SETUP", "ChallengeResponses": { "USERNAME":  
  "[username]" }, "SESSION": "[Session ID from VerifySoftwareToken]"
```

SELECT_MFA_TYPE

```
"ChallengeName": "SELECT_MFA_TYPE", "ChallengeResponses": {"USERNAME": "[username]", "ANSWER": "[SMS_MFA|EMAIL_MFA|SOFTWARE_TOKEN_MFA]"}
```

For more information about SECRET_HASH, see [Computing secret hash values](#). For information about DEVICE_KEY, see [Working with user devices in your user pool](#).

This data type is a request parameter of [RespondToAuthChallenge](#) and [AdminRespondToAuthChallenge](#).

Contents

ChallengeName

The type of challenge that your previous authentication request returned in the parameter ChallengeName, for example SMS_MFA.

Type: String

Valid Values: Password | Mfa

Required: No

ChallengeResponse

The set of key-value pairs that provides a response to the requested challenge.

Type: String

Valid Values: Success | Failure

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](#)

ClientSecretDescriptorType

Contains information about a client secret, including its unique identifier, value, and creation timestamp.

Contents

ClientSecretCreateDate

The date and time when the client secret was created.

Type: Timestamp

Required: No

ClientSecretId

The unique identifier for the client secret. This identifier follows the format <client-id>--<epoch-create-time>.

Type: String

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

Required: No

ClientSecretValue

The actual secret value. This is only returned when creating a new secret and only if Amazon Cognito generated the secret. For custom secrets that you provide, this field is not included in the response.

Type: String

Length Constraints: Minimum length of 24. Maximum length of 64.

Pattern: `[\w+]`

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](#)

ClientSecretListDescriptorType

The metadata of a client secret.

Contents

ClientSecretCreateDate

The date and time when the client secret was created.

Type: Timestamp

Required: No

ClientSecretId

The unique identifier for the client secret.

Type: String

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

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](#)

CloudWatchLogsConfigurationType

Configuration for the CloudWatch log group destination of user pool detailed activity logging, or of user activity log export with threat protection.

This data type is a request parameter of [SetLogDeliveryConfiguration](#) and a response parameter of [GetLogDeliveryConfiguration](#).

Contents

LogGroupArn

The Amazon Resource Name (arn) of a CloudWatch Logs log group where your user pool sends logs. The log group must not be encrypted with AWS Key Management Service and must be in the same AWS account as your user pool.

To send logs to log groups with a resource policy of a size greater than 5120 characters, configure a log group with a path that starts with `/aws/vendedlogs`. For more information, see [Enabling logging from certain AWS services](#).

Type: String

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

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

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](#)

CodeDeliveryDetailsType

The delivery details for an email or SMS message that Amazon Cognito sent for authentication or verification.

This data type is a response parameter of operations that send a code for user profile confirmation, verification, or management, for example [ForgotPassword](#) and [SignUp](#).

Contents

AttributeName

The name of the attribute that Amazon Cognito verifies with the code.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\t\n\r ]+`

Required: No

DeliveryMedium

The method that Amazon Cognito used to send the code.

Type: String

Valid Values: SMS | EMAIL

Required: No

Destination

The email address or phone number destination where Amazon Cognito sent the code.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#)

CompromisedCredentialsActionsType

Settings for user pool actions when Amazon Cognito detects compromised credentials with threat protection in full-function ENFORCED mode.

This data type is a request parameter of [SetRiskConfiguration](#) and a response parameter of [DescribeRiskConfiguration](#).

Contents

EventAction

The action that Amazon Cognito takes when it detects compromised credentials.

Type: String

Valid Values: BLOCK | NO_ACTION

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](#)

CompromisedCredentialsRiskConfigurationType

Settings for compromised-credentials actions and authentication-event sources with threat protection in full-function ENFORCED mode.

This data type is a request parameter of [SetRiskConfiguration](#) and a response parameter of [DescribeRiskConfiguration](#).

Contents

Actions

Settings for the actions that you want your user pool to take when Amazon Cognito detects compromised credentials.

Type: [CompromisedCredentialsActionsType](#) object

Required: Yes

EventFilter

Settings for the sign-in activity where you want to configure compromised-credentials actions. Defaults to all events.

Type: Array of strings

Valid Values: SIGN_IN | PASSWORD_CHANGE | SIGN_UP

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](#)

ContextDataType

Contextual user data used for evaluating the risk of an authentication event by user pool threat protection.

This data type is a request parameter of server-side authentication operations like [AdminInitiateAuth](#) and [AdminRespondToAuthChallenge](#).

Contents

HttpHeaders

The HTTP headers from your user's authentication request.

Type: Array of [HttpHeader](#) objects

Required: Yes

IpAddress

The source IP address of your user's device.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: Yes

ServerName

The name of your application's service endpoint.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: Yes

ServerPath

The path of your application's service endpoint.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: Yes

EncodedData

Encoded device-fingerprint details that your app collected with the Amazon Cognito context data collection library. For more information, see [Adding user device and session data to API requests](#).

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#)

CustomDomainConfigType

The configuration for a hosted UI custom domain.

This data type is a request parameter of [CreateUserPoolDomain](#) and [UpdateUserPoolDomain](#).

Contents

CertificateArn

The Amazon Resource Name (ARN) of an AWS Certificate Manager SSL certificate. You use this certificate for the subdomain of your custom domain.

Type: String

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

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

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](#)

CustomEmailLambdaVersionConfigType

The properties of a custom email sender Lambda trigger.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

LambdaArn

The Amazon Resource Name (ARN) of the function that you want to assign to your Lambda trigger.

Type: String

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

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

Required: Yes

LambdaVersion

The user pool trigger version of the request that Amazon Cognito sends to your Lambda function. Higher-numbered versions add fields that support new features.

You must use a `LambdaVersion` of `V1_0` with a custom sender function.

Type: String

Valid Values: `V1_0`

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](#)

CustomSMSLambdaVersionConfigType

The properties of a custom SMS sender Lambda trigger.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

LambdaArn

The Amazon Resource Name (ARN) of the function that you want to assign to your Lambda trigger.

Type: String

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

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

Required: Yes

LambdaVersion

The user pool trigger version of the request that Amazon Cognito sends to your Lambda function. Higher-numbered versions add fields that support new features.

You must use a `LambdaVersion` of `V1_0` with a custom sender function.

Type: String

Valid Values: `V1_0`

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](#)

DeviceConfigurationType

The device-remembering configuration for a user pool.

A [DescribeUserPool](#) request returns a null value for this object when the user pool isn't configured to remember devices. When device remembering is active, you can remember a user's device with a [ConfirmDevice](#) API request. Additionally, when the property `DeviceOnlyRememberedOnUserPrompt` is true, you must follow `ConfirmDevice` with an [UpdateDeviceStatus](#) API request that sets the user's device to `remembered` or `not_remembered`.

To sign in with a remembered device, include `DEVICE_KEY` in the authentication parameters in your user's [InitiateAuth](#) request. If your app doesn't include a `DEVICE_KEY` parameter, the [InitiateAuth](#) from Amazon Cognito includes newly-generated `DEVICE_KEY` and `DEVICE_GROUP_KEY` values under `NewDeviceMetadata`. Store these values to use in future device-authentication requests.

Note

When you provide a value for any property of `DeviceConfiguration`, you activate the device remembering for the user pool.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

ChallengeRequiredOnNewDevice

When true, a remembered device can sign in with device authentication instead of SMS and time-based one-time password (TOTP) factors for multi-factor authentication (MFA).

Note

Whether or not `ChallengeRequiredOnNewDevice` is true, users who sign in with devices that have not been confirmed or remembered must still provide a second factor in a user pool that requires MFA.

Type: Boolean

Required: No

DeviceOnlyRememberedOnUserPrompt

When true, Amazon Cognito doesn't automatically remember a user's device when your app sends a `ConfirmDevice` API request. In your app, create a prompt for your user to choose whether they want to remember their device. Return the user's choice in an `UpdateDeviceStatus` API request.

When `DeviceOnlyRememberedOnUserPrompt` is false, Amazon Cognito immediately remembers devices that you register in a `ConfirmDevice` API request.

Type: Boolean

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](#)

DeviceSecretVerifierConfigType

A Secure Remote Password (SRP) value that your application generates when you register a user's device. For more information, see [Getting a device key](#).

This data type is a request parameter of [ConfirmDevice](#).

Contents

PasswordVerifier

A password verifier for a user's device. Used in SRP authentication.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

Salt

The salt that you want to use in SRP authentication with the user's device.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#)

DeviceType

Information about a user's device that they've registered for device SRP authentication in your application. For more information, see [Working with user devices in your user pool](#).

This data type is a response parameter of [AdminGetDevice](#), [AdminListDevices](#), and [GetDevice](#).

Contents

DeviceAttributes

Metadata about a user's device, like name and last-access source IP.

Type: Array of [AttributeType](#) objects

Required: No

DeviceCreateDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

DeviceKey

The device key, for example `us-west-2_EXAMPLE-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-f-]+\`

Required: No

DeviceLastAuthenticatedDate

The date when the user last signed in with the device.

Type: Timestamp

Required: No

DeviceLastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

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](#)

DomainDescriptionType

A container for information about the user pool domain associated with the hosted UI and OAuth endpoints.

This data type is a response parameter of [DescribeUserPoolDomain](#).

Contents

AWSAccountId

The AWS account that you created the user pool in.

Type: String

Length Constraints: Maximum length of 12.

Pattern: [0-9]+

Required: No

CloudFrontDistribution

The Amazon CloudFront endpoint that hosts your custom domain.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

CustomDomainConfig

The configuration for a custom domain that hosts the sign-up and sign-in webpages for your application.

Type: [CustomDomainConfigType](#) object

Required: No

Domain

The domain string. For custom domains, this is the fully-qualified domain name, such as `auth.example.com`. For Amazon Cognito prefix domains, this is the prefix alone, such as `auth`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 63.

Pattern: `^[a-z0-9](?:[a-z0-9\-\]{0,61}[a-z0-9])?$`

Required: No

ManagedLoginVersion

The version of managed login branding that you want to apply to your domain. A value of 1 indicates hosted UI (classic) branding and a version of 2 indicates managed login branding.

Managed login requires that your user pool be configured for any [feature plan](#) other than Lite.

Type: Integer

Required: No

S3Bucket

The Amazon S3 bucket where the static files for this domain are stored.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 1024.

Pattern: `^[0-9A-Za-z\.\-\_]*(?<!\. )$`

Required: No

Status

The domain status.

Type: String

Valid Values: CREATING | DELETING | UPDATING | ACTIVE | FAILED

Required: No

UserPoolId

The ID of the user pool that the domain is attached to.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: No

Version

The app version.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 20.

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](#)

EmailConfigurationType

The email configuration of your user pool. The email configuration type sets your preferred sending method, AWS Region, and sender for messages from your user pool.

Note

Amazon Cognito can send email messages with Amazon Simple Email Service resources in the AWS Region where you created your user pool, and in alternate Regions in some cases. For more information on the supported Regions, see [Email settings for Amazon Cognito user pools](#).

This data type is a request parameter of [CreateUserPool](#), [UpdateUserPool](#), and [SetUserPoolMfaConfig](#), and a response parameter of [CreateUserPool](#), [UpdateUserPool](#), and [GetUserPoolMfaConfig](#).

Contents

ConfigurationSet

The set of configuration rules that can be applied to emails sent using Amazon Simple Email Service. A configuration set is applied to an email by including a reference to the configuration set in the headers of the email. Once applied, all of the rules in that configuration set are applied to the email. Configuration sets can be used to apply the following types of rules to emails:

Event publishing

Amazon Simple Email Service can track the number of send, delivery, open, click, bounce, and complaint events for each email sent. Use event publishing to send information about these events to other AWS services such as Amazon CloudWatch.

IP pool management

When leasing dedicated IP addresses with Amazon Simple Email Service, you can create groups of IP addresses, called dedicated IP pools. You can then associate the dedicated IP pools with configuration sets.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[a-zA-Z0-9_-]+$`

Required: No

EmailSendingAccount

Specifies whether Amazon Cognito uses its built-in functionality to send your users email messages, or uses your Amazon Simple Email Service email configuration. Specify one of the following values:

COGNITO_DEFAULT

When Amazon Cognito emails your users, it uses its built-in email functionality. When you use the default option, Amazon Cognito allows only a limited number of emails each day for your user pool. For typical production environments, the default email limit is less than the required delivery volume. To achieve a higher delivery volume, specify DEVELOPER to use your Amazon SES email configuration.

To look up the email delivery limit for the default option, see [Limits](#) in the *Amazon Cognito Developer Guide*.

The default FROM address is `no-reply@verificationemail.com`. To customize the FROM address, provide the Amazon Resource Name (ARN) of an Amazon SES verified email address for the `SourceArn` parameter.

DEVELOPER

When Amazon Cognito emails your users, it uses your Amazon SES configuration. Amazon Cognito calls Amazon SES on your behalf to send email from your verified email address. When you use this option, the email delivery limits are the same limits that apply to your Amazon SES verified email address in your AWS account.

If you use this option, provide the ARN of an Amazon SES verified email address for the `SourceArn` parameter.

Before Amazon Cognito can email your users, it requires additional permissions to call Amazon SES on your behalf. When you update your user pool with this option, Amazon Cognito creates a *service-linked role*, which is a type of role in your AWS account. This role contains the permissions that allow you to access Amazon SES and send email messages from your email address. For more information about the service-linked role that Amazon

Cognito creates, see [Using Service-Linked Roles for Amazon Cognito](#) in the *Amazon Cognito Developer Guide*.

Type: String

Valid Values: COGNITO_DEFAULT | DEVELOPER

Required: No

From

Either the sender's email address or the sender's name with their email address. For example, `testuser@example.com` or `Test User <testuser@example.com>`. This address appears before the body of the email.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ReplyToEmailAddress

The destination to which the receiver of the email should reply.

Type: String

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+@[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: No

SourceArn

The ARN of a verified email address or an address from a verified domain in Amazon SES. You can set a `SourceArn` email from a verified domain only with an API request. You can set a verified email address, but not an address in a verified domain, in the Amazon Cognito console. Amazon Cognito uses the email address that you provide in one of the following ways, depending on the value that you specify for the `EmailSendingAccount` parameter:

- If you specify `COGNITO_DEFAULT`, Amazon Cognito uses this address as the custom FROM address when it emails your users using its built-in email account.
- If you specify `DEVELOPER`, Amazon Cognito emails your users with this address by calling Amazon SES on your behalf.

The Region value of the SourceArn parameter must indicate a supported AWS Region of your user pool. Typically, the Region in the SourceArn and the user pool Region are the same. For more information, see [Amazon SES email configuration regions](#) in the [Amazon Cognito Developer Guide](#).

Type: String

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

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

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](#)

EmailMfaConfigType

Sets or shows configuration for user pool email message MFA and sign-in with one-time passwords (OTPs). Includes the subject and body of the email message template for sign-in and MFA messages. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

This data type is a request parameter of [SetUserPoolMfaConfig](#) and a response parameter of [GetUserPoolMfaConfig](#).

Contents

Message

The template for the email messages that your user pool sends to users with codes for MFA and sign-in with email OTPs. The message must contain the {####} placeholder. In the message, Amazon Cognito replaces this placeholder with the code. If you don't provide this parameter, Amazon Cognito sends messages in the default format.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 20000.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s*]*\{####\}`
`[\p{L}\p{M}\p{S}\p{N}\p{P}\s*]*`

Required: No

Subject

The subject of the email messages that your user pool sends to users with codes for MFA and email OTP sign-in.

Type: String

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s]+`

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](#)

EmailMfaSettingsType

User preferences for multi-factor authentication with email messages. Activates or deactivates email MFA and sets it as the preferred MFA method when multiple methods are available. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

This data type is a request parameter of [SetUserMFAPreference](#) and [AdminSetUserMFAPreference](#).

Contents

Enabled

Specifies whether email message MFA is active for a user. When the value of this parameter is `Enabled`, the user will be prompted for MFA during all sign-in attempts, unless device tracking is turned on and the device has been trusted.

Type: Boolean

Required: No

PreferredMfa

Specifies whether email message MFA is the user's preferred method.

Type: Boolean

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](#)

EventContextDataType

The context data that your application submitted in an authentication request with threat protection, as displayed in an `AdminListUserAuthEvents` response.

Contents

City

The user's city.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

Country

The user's country.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

DeviceName

The user's device name.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

IpAddress

The source IP address of your user's device.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

Timezone

The user's time zone.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#)

EventFeedbackType

The feedback that your application submitted to a threat protection event log, as displayed in an `AdminListUserAuthEvents` response.

Contents

FeedbackValue

Your feedback to the authentication event. When you provide a `FeedbackValue` value of `valid`, you tell Amazon Cognito that you trust a user session where Amazon Cognito has evaluated some level of risk. When you provide a `FeedbackValue` value of `invalid`, you tell Amazon Cognito that you don't trust a user session, or you don't believe that Amazon Cognito evaluated a high-enough risk level.

Type: String

Valid Values: `Valid` | `Invalid`

Required: Yes

Provider

The submitter of the event feedback. For example, if you submit event feedback in the Amazon Cognito console, this value is `Admin`.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: Yes

FeedbackDate

The date that you or your user submitted the feedback.

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](#)

EventRiskType

The risk evaluation by adaptive authentication, as displayed in an `AdminListUserAuthEvents` response. Contains evaluations of compromised-credentials detection and assessed risk level and action taken by adaptive authentication.

Contents

CompromisedCredentialsDetected

Indicates whether compromised credentials were detected during an authentication event.

Type: Boolean

Required: No

RiskDecision

The action taken by adaptive authentication. If `NoRisk`, your user pool took no action. If `AccountTakeover`, your user pool applied the adaptive authentication automated response that you configured. If `Block`, your user pool prevented the attempt.

Type: String

Valid Values: `NoRisk` | `AccountTakeover` | `Block`

Required: No

RiskLevel

The risk level that adaptive authentication assessed for the authentication event.

Type: String

Valid Values: `Low` | `Medium` | `High`

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](#)

FirehoseConfigurationType

Configuration for the Amazon Data Firehose stream destination of user activity log export with threat protection.

Contents

StreamArn

The ARN of an Amazon Data Firehose stream that's the destination for threat protection log export.

Type: String

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

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

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](#)

GroupType

A user pool group. Contains details about the group and the way that it contributes to IAM role decisions with identity pools. Identity pools can make decisions about the IAM role to assign based on groups: users get credentials for the role associated with their highest-priority group.

This data type is a response parameter of [AdminListGroupsForUser](#), [CreateGroup](#), [GetGroup](#), [ListGroups](#), and [UpdateGroup](#).

Contents

CreationDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

Description

A friendly description of the group.

Type: String

Length Constraints: Maximum length of 2048.

Required: No

GroupName

The name of the group.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}] +`

Required: No

LastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

Precedence

A non-negative integer value that specifies the precedence of this group relative to the other groups that a user can belong to in the user pool. Zero is the highest precedence value. Groups with lower Precedence values take precedence over groups with higher or null Precedence values. If a user belongs to two or more groups, it is the group with the lowest precedence value whose role ARN is given in the user's tokens for the `cognito:roles` and `cognito:preferred_role` claims.

Two groups can have the same Precedence value. If this happens, neither group takes precedence over the other. If two groups with the same Precedence have the same role ARN, that role is used in the `cognito:preferred_role` claim in tokens for users in each group. If the two groups have different role ARNs, the `cognito:preferred_role` claim isn't set in users' tokens.

The default Precedence value is `null`.

Type: Integer

Valid Range: Minimum value of 0.

Required: No

RoleArn

The ARN of the IAM role associated with the group. If a group has the highest priority of a user's groups, users who authenticate with an identity pool get credentials for the RoleArn that's associated with the group.

Type: String

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

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

Required: No

UserPoolId

The ID of the user pool that contains the group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#)

HTTPHeader

The HTTP header in the `ContextData` parameter.

This data type is a request parameter of server-side authentication operations like [AdminInitiateAuth](#) and [AdminRespondToAuthChallenge](#).

Contents

headerName

The header name.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

headerValue

The header value.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#)

IdentityProviderType

A user pool identity provider (IdP). Contains information about a third-party IdP to a user pool, the attributes that it populates to user profiles, and the trust relationship between the IdP and your user pool.

This data type is a response parameter of [CreateIdentityProvider](#), [DescribeIdentityProvider](#), [GetIdentityProviderByIdentifier](#), and [UpdateIdentityProvider](#).

Contents

AttributeMapping

A mapping of IdP attributes to standard and custom user pool attributes.

Type: String to string map

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

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

CreationDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

IdpIdentifiers

A list of IdP identifiers. IdP identifiers are strings that represent friendly names or domain names of IdPs, for example MyIdP or auth.example.com. You can choose to route user authorization requests to the right IdP with either IdP identifiers or IdP names. For more information, see `identity_provider` and `idp_identifier` at [Authorize endpoint](#).

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 40.

Pattern: `[\w\s+=.@- ]+`

Required: No

LastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

ProviderDetails

The scopes, URLs, and identifiers for your external identity provider. The following examples describe the provider detail keys for each IdP type. These values and their schema are subject to change. Social IdP `authorize_scopes` values must match the values listed here.

OpenID Connect (OIDC)

Amazon Cognito accepts the following elements when it can't discover endpoint URLs from `oidc_issuer`: `attributes_url`, `authorize_url`, `jwt_uri`, `token_url`.

```
Create or update request: "ProviderDetails": { "attributes_request_method":  
"GET", "attributes_url": "https://auth.example.com/userInfo",  
"authorize_scopes": "openid profile email", "authorize_url": "https://  
auth.example.com/authorize", "client_id": "1example23456789",  
"client_secret": "provider-app-client-secret", "jwt_uri": "https://  
auth.example.com/.well-known/jwks.json", "oidc_issuer": "https://  
auth.example.com", "token_url": "https://example.com/token" }
```

```
Describe response: "ProviderDetails": { "attributes_request_method":  
"GET", "attributes_url": "https://auth.example.com/userInfo",  
"attributes_url_add_attributes": "false", "authorize_scopes": "openid  
profile email", "authorize_url": "https://auth.example.com/authorize",  
"client_id": "1example23456789", "client_secret": "provider-app-
```

```
client-secret", "jwks_uri": "https://auth.example.com/.well-known/
jwks.json", "oidc_issuer": "https://auth.example.com", "token_url":
"https://example.com/token" }
```

SAML

Create or update request with Metadata URL: "ProviderDetails": { "IDPInit": "true", "IDPSignout": "true", "EncryptedResponses" : "true", "MetadataURL": "https://auth.example.com/sso/saml/metadata", "RequestSigningAlgorithm": "rsa-sha256" }

Create or update request with Metadata file: "ProviderDetails": { "IDPInit": "true", "IDPSignout": "true", "EncryptedResponses" : "true", "MetadataFile": "[metadata XML]", "RequestSigningAlgorithm": "rsa-sha256" }

The value of MetadataFile must be the plaintext metadata document with all quote (") characters escaped by backslashes.

Describe response: "ProviderDetails": { "IDPInit": "true", "IDPSignout": "true", "EncryptedResponses" : "true", "ActiveEncryptionCertificate": "[certificate]", "MetadataURL": "https://auth.example.com/sso/saml/metadata", "RequestSigningAlgorithm": "rsa-sha256", "SLORedirectBindingURI": "https://auth.example.com/slo/saml", "SSORedirectBindingURI": "https://auth.example.com/sso/saml" }

LoginWithAmazon

Create or update request: "ProviderDetails": { "authorize_scopes": "profile postal_code", "client_id": "amzn1.application-oa2-client.1example23456789", "client_secret": "provider-app-client-secret"

Describe response: "ProviderDetails": { "attributes_url": "https://api.amazon.com/user/profile", "attributes_url_add_attributes": "false", "authorize_scopes": "profile postal_code", "authorize_url": "https://www.amazon.com/ap/oa", "client_id": "amzn1.application-oa2-client.1example23456789", "client_secret": "provider-app-client-secret", "token_request_method": "POST", "token_url": "https://api.amazon.com/auth/o2/token" }

Google

Create or update request: "ProviderDetails": { "authorize_scopes": "email profile openid", "client_id": "1example23456789.apps.googleusercontent.com", "client_secret": "provider-app-client-secret" }

Describe response: "ProviderDetails": { "attributes_url": "https://people.googleapis.com/v1/people/me?personFields=", "attributes_url_add_attributes": "true", "authorize_scopes": "email profile openid", "authorize_url": "https://accounts.google.com/o/oauth2/v2/auth", "client_id": "1example23456789.apps.googleusercontent.com", "client_secret": "provider-app-client-secret", "oidc_issuer": "https://accounts.google.com", "token_request_method": "POST", "token_url": "https://www.googleapis.com/oauth2/v4/token" }

SignInWithApple

Create or update request: "ProviderDetails": { "authorize_scopes": "email name", "client_id": "com.example.cognito", "private_key": "1EXAMPLE", "key_id": "2EXAMPLE", "team_id": "3EXAMPLE" }

Describe response: "ProviderDetails": { "attributes_url_add_attributes": "false", "authorize_scopes": "email name", "authorize_url": "https://appleid.apple.com/auth/authorize", "client_id": "com.example.cognito", "key_id": "1EXAMPLE", "oidc_issuer": "https://appleid.apple.com", "team_id": "2EXAMPLE", "token_request_method": "POST", "token_url": "https://appleid.apple.com/auth/token" }

Facebook

Create or update request: "ProviderDetails": { "api_version": "v17.0", "authorize_scopes": "public_profile, email", "client_id": "1example23456789", "client_secret": "provider-app-client-secret" }

Describe response: "ProviderDetails": { "api_version": "v17.0", "attributes_url": "https://graph.facebook.com/v17.0/me?fields=", "attributes_url_add_attributes": "true", "authorize_scopes": "public_profile, email", "authorize_url": "https://www.facebook.com/"

```
v17.0/dialog/oauth", "client_id": "1example23456789", "client_secret":  
"provider-app-client-secret", "token_request_method": "GET",  
"token_url": "https://graph.facebook.com/v17.0/oauth/access_token" }
```

Type: String to string map

Key Length Constraints: Minimum length of 0. Maximum length of 131072.

Value Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ProviderName

A friendly name for the IdP.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\p{Z}]+`

Required: No

ProviderType

The type of IdP. Either SAML, OIDC, or a named social identity provider.

Type: String

Valid Values: SAML | Facebook | Google | LoginWithAmazon | SignInWithApple |
OIDC

Required: No

UserPoolId

The ID of the user pool associated with the IdP.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

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](#)

InboundFederationLambdaType

The properties of an inbound federation Lambda trigger.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

LambdaArn

The Amazon Resource Name (ARN) of the function that you want to assign to your Lambda trigger.

Type: String

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

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

Required: Yes

LambdaVersion

The user pool trigger version of the request that Amazon Cognito sends to your Lambda function. Higher-numbered versions add fields that support new features.

You must use a `LambdaVersion` of `V1_0` with an inbound federation function.

Type: String

Valid Values: `V1_0`

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](#)

LambdaConfigType

A collection of user pool Lambda triggers. Amazon Cognito invokes triggers at several possible stages of user pool operations. Triggers can modify the outcome of the operations that invoked them.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

CreateAuthChallenge

The configuration of a create auth challenge Lambda trigger, one of three triggers in the sequence of the [custom authentication challenge triggers](#).

Type: String

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

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

Required: No

CustomEmailSender

The configuration of a custom email sender Lambda trigger. This trigger routes all email notifications from a user pool to a Lambda function that delivers the message using custom logic.

Type: [CustomEmailLambdaVersionConfigType](#) object

Required: No

CustomMessage

A custom message Lambda trigger. This trigger is an opportunity to customize all SMS and email messages from your user pool. When a custom message trigger is active, your user pool routes all messages to a Lambda function that returns a runtime-customized message subject and body for your user pool to deliver to a user.

Type: String

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

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

Required: No

CustomSMSSender

The configuration of a custom SMS sender Lambda trigger. This trigger routes all SMS notifications from a user pool to a Lambda function that delivers the message using custom logic.

Type: [CustomSMSLambdaVersionConfigType](#) object

Required: No

DefineAuthChallenge

The configuration of a define auth challenge Lambda trigger, one of three triggers in the sequence of the [custom authentication challenge triggers](#).

Type: String

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

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

Required: No

InboundFederation

The configuration of an inbound federation Lambda trigger. This trigger can transform federated user attributes during the authentication with external identity providers.

Type: [InboundFederationLambdaType](#) object

Required: No

KMSKeyID

The ARN of an [KMS key](#). Amazon Cognito uses the key to encrypt codes and temporary passwords sent to custom sender Lambda triggers.

Type: String

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

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

Required: No

PostAuthentication

The configuration of a [post authentication Lambda trigger](#) in a user pool. This trigger can take custom actions after a user signs in.

Type: String

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

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

Required: No

PostConfirmation

The configuration of a [post confirmation Lambda trigger](#) in a user pool. This trigger can take custom actions after a user confirms their user account and their email address or phone number.

Type: String

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

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

Required: No

PreAuthentication

The configuration of a [pre authentication trigger](#) in a user pool. This trigger can evaluate and modify user sign-in events.

Type: String

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

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

Required: No

PreSignUp

The configuration of a [pre sign-up Lambda trigger](#) in a user pool. This trigger evaluates new users and can bypass confirmation, [link a federated user profile](#), or block sign-up requests.

Type: String

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

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

Required: No

PreTokenGeneration

The legacy configuration of a [pre token generation Lambda trigger](#) in a user pool.

Set this parameter for legacy purposes. If you also set an ARN in `PreTokenGenerationConfig`, its value must be identical to `PreTokenGeneration`. For new instances of pre token generation triggers, set the `LambdaArn` of `PreTokenGenerationConfig`.

Type: String

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

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

Required: No

PreTokenGenerationConfig

The detailed configuration of a [pre token generation Lambda trigger](#) in a user pool. If you also set an ARN in `PreTokenGeneration`, its value must be identical to `PreTokenGenerationConfig`.

Type: [PreTokenGenerationVersionConfigType](#) object

Required: No

UserMigration

The configuration of a [migrate user Lambda trigger](#) in a user pool. This trigger can create user profiles when users sign in or attempt to reset their password with credentials that don't exist yet.

Type: String

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

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

Required: No

VerifyAuthChallengeResponse

The configuration of a verify auth challenge Lambda trigger, one of three triggers in the sequence of the [custom authentication challenge triggers](#).

Type: String

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

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

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](#)

LogConfigurationType

The configuration of user event logs to an external AWS service like Amazon Data Firehose, Amazon S3, or Amazon CloudWatch Logs.

This data type is a request parameter of [SetLogDeliveryConfiguration](#) and a response parameter of [GetLogDeliveryConfiguration](#).

Contents

EventSource

The source of events that your user pool sends for logging. To send error-level logs about user notification activity, set to `userNotification`. To send info-level logs about threat-protection user activity in user pools with the Plus feature plan, set to `userAuthEvents`.

Type: String

Valid Values: `userNotification` | `userAuthEvents`

Required: Yes

LogLevel

The `errorlevel` selection of logs that a user pool sends for detailed activity logging. To send `userNotification` activity with [information about message delivery](#), choose `ERROR` with `CloudWatchLogsConfiguration`. To send `userAuthEvents` activity with user logs from threat protection with the Plus feature plan, choose `INFO` with one of `CloudWatchLogsConfiguration`, `FirehoseConfiguration`, or `S3Configuration`.

Type: String

Valid Values: `ERROR` | `INFO`

Required: Yes

CloudWatchLogsConfiguration

The CloudWatch log group destination of user pool detailed activity logs, or of user activity log export with threat protection.

Type: [CloudWatchLogsConfigurationType](#) object

Required: No

FirehoseConfiguration

The Amazon Data Firehose stream destination of user activity log export with threat protection. To activate this setting, your user pool must be on the [Plus tier](#).

Type: [FirehoseConfigurationType](#) object

Required: No

S3Configuration

The Amazon S3 bucket destination of user activity log export with threat protection. To activate this setting, your user pool must be on the [Plus tier](#).

Type: [S3ConfigurationType](#) 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](#)

LogDeliveryConfigurationType

The logging parameters of a user pool, as returned in the response to a `GetLogDeliveryConfiguration` request.

Contents

LogConfigurations

A logging destination of a user pool. User pools can have multiple logging destinations for message-delivery and user-activity logs.

Type: Array of [LogConfigurationType](#) objects

Array Members: Minimum number of 0 items. Maximum number of 2 items.

Required: Yes

UserPoolId

The ID of the user pool where you configured logging.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#)

ManagedLoginBrandingType

A managed login branding style that's assigned to a user pool app client.

This data type is a response parameter of [CreateManagedLoginBranding](#), [UpdateManagedLoginBranding](#), [DescribeManagedLoginBranding](#), and [DescribeManagedLoginBrandingByClient](#).

Contents

Assets

An array of image files that you want to apply to roles like backgrounds, logos, and icons. Each object must also indicate whether it is for dark mode, light mode, or browser-adaptive mode.

Type: Array of [AssetType](#) objects

Array Members: Minimum number of 0 items. Maximum number of 40 items.

Required: No

CreationDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

LastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

ManagedLoginBrandingId

The ID of the managed login branding style.

Type: String

Pattern: `^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[4][0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}$`

Required: No

Settings

A JSON file, encoded as a Document type, with the the settings that you want to apply to your style.

The following components are not currently implemented and reserved for future use:

- `signUp`
- `instructions`
- `sessionTimerDisplay`
- `languageSelector` (for localization, see [Managed login localization](#))

Type: JSON value

Required: No

UseCognitoProvidedValues

When true, applies the default branding style options. This option reverts to default style options that are managed by Amazon Cognito. You can modify them later in the branding editor.

When you specify `true` for this option, you must also omit values for `Settings` and `Assets` in the request.

Type: Boolean

Required: No

UserPoolId

The user pool where the branding style is assigned.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#)

MessageTemplateType

The message template structure.

Contents

EmailMessage

The message template for email messages. EmailMessage is allowed only if [EmailSendingAccount](#) is DEVELOPER.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 20000.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s]*`

Required: No

EmailSubject

The subject line for email messages. EmailSubject is allowed only if [EmailSendingAccount](#) is DEVELOPER.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 140.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s]+`

Required: No

SMSMessage

The message template for SMS messages.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 140.

Pattern: `(?s).*`

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](#)

MFAOptionType

This data type is no longer supported. Applies only to SMS multi-factor authentication (MFA) configurations. Does not apply to time-based one-time password (TOTP) software token MFA configurations.

To set either type of MFA configuration, use the [AdminSetUserMFAPreference](#) or [SetUserMFAPreference](#) actions.

To look up information about either type of MFA configuration, use the [AdminGetUser:UserMFASettingList](#) or [GetUser:UserMFASettingList](#) responses.

Contents

AttributeName

The attribute name of the MFA option type. The only valid value is phone_number.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\t\n\r ]+`

Required: No

DeliveryMedium

The delivery medium to send the MFA code. You can use this parameter to set only the SMS delivery medium value.

Type: String

Valid Values: SMS | EMAIL

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](#)

NewDeviceMetadataType

Information that your user pool responds with in `AuthenticationResult` when you configure it to remember devices and a user signs in with an unrecognized device. Amazon Cognito presents a new device key that you can use to set up [device authentication](#) in a "Remember me on this device" authentication model.

This data type is a response parameter of authentication operations like [InitiateAuth](#), [AdminInitiateAuth](#), [RespondToAuthChallenge](#), and [AdminRespondToAuthChallenge](#).

Contents

DeviceGroupKey

The device group key, an identifier used in generating the `DEVICE_PASSWORD_VERIFIER` for device SRP authentication.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

DeviceKey

The device key, an identifier used in generating the `DEVICE_PASSWORD_VERIFIER` for device SRP authentication.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-f-]+`

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](#)

NotifyConfigurationType

The configuration for Amazon SES email messages that threat protection sends to a user when your adaptive authentication automated response has a *Notify* action.

This data type is a request parameter of [SetRiskConfiguration](#) and a response parameter of [DescribeRiskConfiguration](#).

Contents

SourceArn

The Amazon Resource Name (ARN) of the identity that is associated with the sending authorization policy. This identity permits Amazon Cognito to send for the email address specified in the From parameter.

Type: String

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

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

Required: Yes

BlockEmail

The template for the email message that your user pool sends when a detected risk event is blocked.

Type: [NotifyEmailType](#) object

Required: No

From

The email address that sends the email message. The address must be either individually verified with Amazon Simple Email Service, or from a domain that has been verified with Amazon SES.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

MfaEmail

The template for the email message that your user pool sends when MFA is challenged in response to a detected risk.

Type: [NotifyEmailType](#) object

Required: No

NoActionEmail

The template for the email message that your user pool sends when no action is taken in response to a detected risk.

Type: [NotifyEmailType](#) object

Required: No

ReplyTo

The reply-to email address of an email template. Can be an email address in the format `admin@example.com` or `Administrator <admin@example.com>`.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#)

NotifyEmailType

The template for email messages that threat protection sends to a user when your threat protection automated response has a *Notify* action.

This data type is a request parameter of [SetRiskConfiguration](#) and a response parameter of [DescribeRiskConfiguration](#).

Contents

Subject

The subject of the threat protection email notification.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 140.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s]+`

Required: Yes

HtmlBody

The body of an email notification formatted in HTML. Choose an `HtmlBody` or a `TextBody` to send an HTML-formatted or plaintext message, respectively.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 20000.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s*]+`

Required: No

TextBody

The body of an email notification formatted in plaintext. Choose an `HtmlBody` or a `TextBody` to send an HTML-formatted or plaintext message, respectively.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 20000.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s*]+`

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](#)

NumberAttributeConstraintsType

The minimum and maximum values of an attribute that is of the number type, for example `custom:age`.

This data type is part of [SchemaAttributeType](#). It defines the length constraints on number-type attributes that you configure in [CreateUserPool](#) and [UpdateUserPool](#), and displays the length constraints of all number-type attributes in the response to [DescribeUserPool](#)

Contents

MaxValue

The maximum length of a number attribute value. Must be a number less than or equal to 2^{1023} , represented as a string with a length of 131072 characters or fewer.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

MinValue

The minimum value of an attribute that is of the number data type.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#)

PasswordPolicyType

The password policy settings for a user pool, including complexity, history, and length requirements.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

MinimumLength

The minimum length of the password in the policy that you have set. This value can't be less than 6.

Type: Integer

Valid Range: Minimum value of 6. Maximum value of 99.

Required: No

PasswordHistorySize

The number of previous passwords that you want Amazon Cognito to restrict each user from reusing. Users can't set a password that matches any of n previous passwords, where n is the value of PasswordHistorySize.

Password history isn't enforced and isn't displayed in [DescribeUserPool](#) responses when you set this value to 0 or don't provide it. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 24.

Required: No

RequireLowercase

The requirement in a password policy that users must include at least one lowercase letter in their password.

Type: Boolean

Required: No

RequireNumbers

The requirement in a password policy that users must include at least one number in their password.

Type: Boolean

Required: No

RequireSymbols

The requirement in a password policy that users must include at least one symbol in their password.

Type: Boolean

Required: No

RequireUppercase

The requirement in a password policy that users must include at least one uppercase letter in their password.

Type: Boolean

Required: No

TemporaryPasswordValidityDays

The number of days a temporary password is valid in the password policy. If the user doesn't sign in during this time, an administrator must reset their password. Defaults to 7. If you submit a value of 0, Amazon Cognito treats it as a null value and sets TemporaryPasswordValidityDays to its default value.

Note

When you set TemporaryPasswordValidityDays for a user pool, you can no longer set a value for the legacy UnusedAccountValidityDays parameter in that user pool.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 365.

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](#)

PreTokenGenerationVersionConfigType

The properties of a pre token generation Lambda trigger.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

LambdaArn

The Amazon Resource Name (ARN) of the function that you want to assign to your Lambda trigger.

This parameter and the `PreTokenGeneration` property of `LambdaConfig` have the same value. For new instances of pre token generation triggers, set `LambdaArn`.

Type: String

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

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

Required: Yes

LambdaVersion

The user pool trigger version of the request that Amazon Cognito sends to your Lambda function. Higher-numbered versions add fields that support new features.

Type: String

Valid Values: `V1_0` | `V2_0` | `V3_0`

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](#)

ProviderDescription

The details of a user pool identity provider (IdP), including name and type.

This data type is a response parameter of [ListIdentityProviders](#).

Contents

CreationDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

LastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

ProviderName

The name of the IdP, for example MySAMLProvider.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\p{Z}]+`

Required: No

ProviderType

The type of the provider, for example SAML. Amazon Cognito supports SAML 2.0, OIDC, and social IdPs. User pools list supported social IdPs by name in this response parameter: Facebook, Google, Login with Amazon, and Sign in with Apple.

Type: String

Valid Values: SAML | Facebook | Google | LoginWithAmazon | SignInWithApple |
OIDC

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](#)

ProviderUserIdentifierType

The characteristics of a source or destination user for linking a federated user profile to a local user profile.

This data type is a request parameter of [AdminLinkProviderForUser](#) and [AdminDisableProviderForUser](#).

Contents

ProviderAttributeName

The name of the provider attribute to link to, such as NameID.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ProviderAttributeValue

The value of the provider attribute to link to, such as xxxxx_account.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

ProviderName

The name of the provider, such as Facebook, Google, or Login with Amazon.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\p{Z}]`+

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](#)

RecoveryOptionType

A recovery option for a user. The `AccountRecoverySettingType` data type is an array of this object. Each `RecoveryOptionType` has a `priority` property that determines whether it is a primary or secondary option.

For example, if `verified_email` has a priority of 1 and `verified_phone_number` has a priority of 2, your user pool sends account-recovery messages to a verified email address but falls back to an SMS message if the user has a verified phone number. The `admin_only` option prevents self-service account recovery.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

Name

The recovery method that this object sets a recovery option for.

Type: String

Valid Values: `verified_email` | `verified_phone_number` | `admin_only`

Required: Yes

Priority

Your priority preference for using the specified attribute in account recovery. The highest priority is 1.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 2.

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](#)

RefreshTokenRotationType

The configuration of your app client for refresh token rotation. When enabled, your app client issues new ID, access, and refresh tokens when users renew their sessions with refresh tokens. When disabled, token refresh issues only ID and access tokens.

Refresh token rotation must be completed with [GetTokensFromRefreshToken](#). With refresh token rotation disabled, you can complete token refresh with `GetTokensFromRefreshToken` and with `REFRESH_TOKEN_AUTH` in [InitiateAuth:AuthFlow](#) and [AdminInitiateAuth:AuthFlow](#).

This data type is a request parameter of [CreateUserPoolClient](#) and [UpdateUserPoolClient](#), and a response parameter of [DescribeUserPoolClient](#).

Contents

Feature

The state of refresh token rotation for the current app client.

Type: String

Valid Values: ENABLED | DISABLED

Required: Yes

RetryGracePeriodSeconds

When you request a token refresh with `GetTokensFromRefreshToken`, the original refresh token that you're rotating out can remain valid for a period of time of up to 60 seconds. This allows for client-side retries. When `RetryGracePeriodSeconds` is 0, the grace period is disabled and a successful request immediately invalidates the submitted refresh token.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 60.

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](#)

ResourceServerScopeType

One custom scope associated with a user pool resource server. This data type is a member of ResourceServerScopeType. For more information, see [Scopes, M2M, and API authorization with resource servers](#).

This data type is a request parameter of [CreateResourceServer](#) and a response parameter of [DescribeResourceServer](#).

Contents

ScopeDescription

A friendly description of a custom scope.

Type: String

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

Required: Yes

ScopeName

The name of the scope. Amazon Cognito renders custom scopes in the format resourceServerIdentifier/ScopeName. For example, if this parameter is exampleScope in the resource server with the identifier exampleResourceServer, you request and receive the scope exampleResourceServer/exampleScope.

Type: String

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

Pattern: `[\x21\x23-\x2E\x30-\x5B\x5D-\x7E]+`

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](#)

ResourceServerType

The details of a resource server configuration and associated custom scopes in a user pool.

This data type is a request parameter of [CreateResourceServer](#) and a response parameter of [DescribeResourceServer](#).

Contents

Identifier

A unique resource server identifier for the resource server. The identifier can be an API friendly name like `solar-system-data`. You can also set an API URL like `https://solar-system-data-api.example.com` as your identifier.

Amazon Cognito represents scopes in the access token in the format `$resource-server-identifier/$scope`. Longer scope-identifier strings increase the size of your access tokens.

Type: String

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

Pattern: `[\x21\x23-\x5B\x5D-\x7E]+`

Required: No

Name

The name of the resource server.

Type: String

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

Pattern: `[\w\s+=, .@- ]+`

Required: No

Scopes

A list of scopes that are defined for the resource server.

Type: Array of [ResourceServerScopeType](#) objects

Array Members: Maximum number of 100 items.

Required: No

UserPoolId

The ID of the user pool that contains the resource server configuration.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#)

RiskConfigurationType

The settings of risk configuration for threat protection with threat protection in a user pool.

This data type is a response parameter of [DescribeRiskConfiguration](#) and [SetRiskConfiguration](#).

Contents

AccountTakeoverRiskConfiguration

The settings for automated responses and notification templates for adaptive authentication with threat protection.

Type: [AccountTakeoverRiskConfigurationType](#) object

Required: No

ClientId

The app client where this configuration is applied. When this parameter isn't present, the risk configuration applies to all user pool app clients that don't have client-level settings.

Type: String

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

Pattern: `[\w+]`

Required: No

CompromisedCredentialsRiskConfiguration

Settings for compromised-credentials actions and authentication types with threat protection in full-function ENFORCED mode.

Type: [CompromisedCredentialsRiskConfigurationType](#) object

Required: No

LastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

RiskExceptionConfiguration

Exceptions to the risk evaluation configuration, including always-allow and always-block IP address ranges.

Type: [RiskExceptionConfigurationType](#) object

Required: No

UserPoolId

The ID of the user pool that has the risk configuration applied.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#)

RiskExceptionConfigurationType

Exceptions to the risk evaluation configuration, including always-allow and always-block IP address ranges.

This data type is a request parameter of [SetRiskConfiguration](#) and a response parameter of [DescribeRiskConfiguration](#).

Contents

BlockedIPRangeList

An always-block IP address list. Overrides the risk decision and always blocks authentication requests. This parameter is displayed and set in CIDR notation.

Type: Array of strings

Array Members: Maximum number of 200 items.

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

SkippedIPRangeList

An always-allow IP address list. Risk detection isn't performed on the IP addresses in this range list. This parameter is displayed and set in CIDR notation.

Type: Array of strings

Array Members: Maximum number of 200 items.

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#)

S3ConfigurationType

Configuration for the Amazon S3 bucket destination of user activity log export with threat protection.

Contents

BucketArn

The ARN of an Amazon S3 bucket that's the destination for threat protection log export.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 1024.

Pattern: `arn:[\w+=/,.@-]+:[\w+=/,.@-]+::[\w+=/,.@-]+(:[\w+=/,.@-]+)?(:[\w+=/,.@-]+)?`

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](#)

SchemaAttributeType

A list of the user attributes and their properties in your user pool. The attribute schema contains standard attributes, custom attributes with a `custom:` prefix, and developer attributes with a `dev:` prefix. For more information, see [User pool attributes](#).

Developer-only `dev:` attributes are a legacy feature of user pools, and are read-only to all app clients. You can create and update developer-only attributes only with IAM-authenticated API operations. Use app client read/write permissions instead.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

AttributeDataType

The data format of the values for your attribute. When you choose an `AttributeDataType`, Amazon Cognito validates the input against the data type. A custom attribute value in your user's ID token is always a string, for example `"custom:isMember" : "true"` or `"custom:YearsAsMember" : "12"`.

Type: String

Valid Values: String | Number | DateTime | Boolean

Required: No

DeveloperOnlyAttribute

Note

You should use [WriteAttributes](#) in the user pool client to control how attributes can be mutated for new use cases instead of using `DeveloperOnlyAttribute`.

Specifies whether the attribute type is developer only. This attribute can only be modified by an administrator. Users won't be able to modify this attribute using their access token. For example, `DeveloperOnlyAttribute` can be modified using `AdminUpdateUserAttributes` but can't be updated using `UpdateUserAttributes`.

Type: Boolean

Required: No

Mutable

Specifies whether the value of the attribute can be changed.

Any user pool attribute whose value you map from an IdP attribute must be mutable, with a parameter value of `true`. Amazon Cognito updates mapped attributes when users sign in to your application through an IdP. If an attribute is immutable, Amazon Cognito throws an error when it attempts to update the attribute. For more information, see [Specifying Identity Provider Attribute Mappings for Your User Pool](#).

Type: Boolean

Required: No

Name

The name of your user pool attribute. When you create or update a user pool, adding a schema attribute creates a custom or developer-only attribute. When you add an attribute with a `Name` value of `MyAttribute`, Amazon Cognito creates the custom attribute `custom:MyAttribute`. When `DeveloperOnlyAttribute` is `true`, Amazon Cognito creates your attribute as `dev:MyAttribute`. In an operation that describes a user pool, Amazon Cognito returns this value as `value` for standard attributes, `custom:value` for custom attributes, and `dev:value` for developer-only attributes..

Type: String

Length Constraints: Minimum length of 1. Maximum length of 20.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: No

NumberAttributeConstraints

Specifies the constraints for an attribute of the number type.

Type: [NumberAttributeConstraintsType](#) object

Required: No

Required

Specifies whether a user pool attribute is required. If the attribute is required and the user doesn't provide a value, registration or sign-in will fail.

Type: Boolean

Required: No

StringAttributeConstraints

Specifies the constraints for an attribute of the string type.

Type: [StringAttributeConstraintsType](#) 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](#)

SignInPolicyType

The policy for allowed types of authentication in a user pool. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

AllowedFirstAuthFactors

The sign-in methods that a user pool supports as the first factor. You can permit users to start authentication with a standard username and password, or with other one-time password and hardware factors.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 4 items.

Valid Values: PASSWORD | EMAIL_OTP | SMS_OTP | WEB_AUTHN

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](#)

SmsConfigurationType

User pool configuration for delivery of SMS messages with Amazon Simple Notification Service. To send SMS messages with Amazon SNS in the AWS Region that you want, the Amazon Cognito user pool uses an AWS Identity and Access Management (IAM) role in your AWS account.

This data type is a request parameter of [CreateUserPool](#), [UpdateUserPool](#), and [SetUserPoolMfaConfig](#), and a response parameter of [CreateUserPool](#), [UpdateUserPool](#), and [GetUserPoolMfaConfig](#).

Contents

SnsCallerArn

The Amazon Resource Name (ARN) of the Amazon SNS caller. This is the ARN of the IAM role in your AWS account that Amazon Cognito will use to send SMS messages. SMS messages are subject to a [spending limit](#).

Type: String

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

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

Required: Yes

ExternalId

The external ID provides additional security for your IAM role. You can use an `ExternalId` with the IAM role that you use with Amazon SNS to send SMS messages for your user pool. If you provide an `ExternalId`, your Amazon Cognito user pool includes it in the request to assume your IAM role. You can configure the role trust policy to require that Amazon Cognito, and any principal, provide the `ExternalId`. If you use the Amazon Cognito Management Console to create a role for SMS multi-factor authentication (MFA), Amazon Cognito creates a role with the required permissions and a trust policy that demonstrates use of the `ExternalId`.

For more information about the `ExternalId` of a role, see [How to use an external ID when granting access to your AWS resources to a third party](#).

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

SnsRegion

The AWS Region to use with Amazon SNS integration. You can choose the same Region as your user pool, or a supported **Legacy Amazon SNS alternate Region**.

Amazon Cognito resources in the Asia Pacific (Seoul) AWS Region must use your Amazon SNS configuration in the Asia Pacific (Tokyo) Region. For more information, see [SMS message settings for Amazon Cognito user pools](#).

Type: String

Length Constraints: Minimum length of 5. Maximum length of 32.

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](#)

SmsMfaConfigType

The configuration of multi-factor authentication (MFA) with SMS messages in a user pool.

This data type is a request parameter of [SetUserPoolMfaConfig](#) and a response parameter of [GetUserPoolMfaConfig](#).

Contents

SmsAuthenticationMessage

The SMS authentication message that will be sent to users with the code they must sign in with. The message must contain the {####} placeholder. Your user pool replaces the placeholder with the MFA code. If this parameter isn't provided, your user pool sends a default message.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 140.

Pattern: `.*\{####\}.*`

Required: No

SmsConfiguration

User pool configuration for delivery of SMS messages with Amazon Simple Notification Service. To send SMS messages with Amazon SNS in the AWS Region that you want, the Amazon Cognito user pool uses an AWS Identity and Access Management (IAM) role in your AWS account.

You can set `SmsConfiguration` in `CreateUserPool` and `UpdateUserPool`, or in `SetUserPoolMfaConfig`.

Type: [SmsConfigurationType](#) 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](#)

SMSMfaSettingsType

A user's preference for using SMS message multi-factor authentication (MFA). Turns SMS MFA on and off, and can set SMS as preferred when other MFA options are available. You can't turn off SMS MFA for any of your users when MFA is required in your user pool; you can only set the type that your user prefers.

This data type is a request parameter of [SetUserMFAPreference](#) and [AdminSetUserMFAPreference](#).

Contents

Enabled

Specifies whether SMS message MFA is activated. If an MFA type is activated for a user, the user will be prompted for MFA during all sign-in attempts, unless device tracking is turned on and the device has been trusted.

Type: Boolean

Required: No

PreferredMfa

Specifies whether SMS is the preferred MFA method. If true, your user pool prompts the specified user for a code delivered by SMS message after username-password sign-in succeeds.

Type: Boolean

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](#)

SoftwareTokenMfaConfigType

Settings for time-based one-time password (TOTP) multi-factor authentication (MFA) in a user pool. Enables and disables availability of this feature.

This data type is a request parameter of [SetUserPoolMfaConfig](#) and a response parameter of [GetUserPoolMfaConfig](#).

Contents

Enabled

The activation state of TOTP MFA.

Type: Boolean

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](#)

SoftwareTokenMfaSettingsType

A user's preference for using time-based one-time password (TOTP) multi-factor authentication (MFA). Turns TOTP MFA on and off, and can set TOTP as preferred when other MFA options are available. You can't turn off TOTP MFA for any of your users when MFA is required in your user pool; you can only set the type that your user prefers.

This data type is a request parameter of [SetUserMFAPreference](#) and [AdminSetUserMFAPreference](#).

Contents

Enabled

Specifies whether software token MFA is activated. If an MFA type is activated for a user, the user will be prompted for MFA during all sign-in attempts, unless device tracking is turned on and the device has been trusted.

Type: Boolean

Required: No

PreferredMfa

Specifies whether software token MFA is the preferred MFA method.

Type: Boolean

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](#)

StringAttributeConstraintsType

The minimum and maximum length values of an attribute that is of the string type, for example `custom:department`.

This data type is part of [SchemaAttributeType](#). It defines the length constraints on string-type attributes that you configure in [CreateUserPool](#) and [UpdateUserPool](#), and displays the length constraints of all string-type attributes in the response to [DescribeUserPool](#)

Contents

MaxLength

The maximum length of a string attribute value. Must be a number less than or equal to 2^{1023} , represented as a string with a length of 131072 characters or fewer.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

MinLength

The minimum length of a string attribute value.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#)

TermsDescriptionType

The details of a set of terms documents. For more information, see [Terms documents](#).

This data type is a response parameter of [ListTerms](#).

Contents

CreationDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: Yes

Enforcement

This parameter is reserved for future use and currently accepts one value.

Type: String

Valid Values: NONE

Required: Yes

LastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: Yes

TermsId

The ID of the requested terms documents.

Type: String

Pattern: `^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[4][0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}$`

Required: Yes

TermsName

The type and friendly name of the requested terms documents.

Type: String

Pattern: `^(terms-of-use|privacy-policy)$`

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](#)

TermsType

The details of a set of terms documents. For more information, see [Terms documents](#).

This data type is a response parameter of [CreateTerms](#) and [UpdateTerms](#).

Contents

ClientId

The ID of the app client that the terms documents are assigned to.

Type: String

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

Pattern: `[\w+]`

Required: Yes

CreationDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: Yes

Enforcement

This parameter is reserved for future use and currently accepts one value.

Type: String

Valid Values: NONE

Required: Yes

LastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: Yes

Links

A map of URLs to languages. For each localized language that will view the requested TermsName, assign a URL. A selection of `cognito:default` displays for all languages that don't have a language-specific URL.

For example, `"cognito:default": "https://terms.example.com"`,
`"cognito:spanish": "https://terms.example.com/es"`.

Type: String to string map

Map Entries: Maximum number of 12 items.

Key Pattern: `^cognito:(default|english|french|spanish|german|bahasa-indonesia|italian|japanese|korean|portuguese-brazil|chinese-(simplified|traditional))$`

Value Length Constraints: Minimum length of 1. Maximum length of 1024.

Value Pattern: `^[\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}]+$`

Required: Yes

TermsId

The ID of the terms documents.

Type: String

Pattern: `^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[4][0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}$`

Required: Yes

TermsName

The type and friendly name of the terms documents.

Type: String

Pattern: `^(terms-of-use|privacy-policy)$`

Required: Yes

TermsSource

This parameter is reserved for future use and currently accepts one value.

Type: String

Valid Values: LINK

Required: Yes

UserPoolId

The ID of the user pool that contains the terms documents.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#)

TokenValidityUnitsType

The time units that, with `IdTokenValidity`, `AccessTokenValidity`, and `RefreshTokenValidity`, set and display the duration of ID, access, and refresh tokens for an app client. You can assign a separate token validity unit to each type of token.

This data type is a request parameter of [CreateUserPoolClient](#) and [UpdateUserPoolClient](#), and a response parameter of [DescribeUserPoolClient](#).

Contents

AccessToken

A time unit for the value that you set in the `AccessTokenValidity` parameter. The default `AccessTokenValidity` time unit is hours. `AccessTokenValidity` duration can range from five minutes to one day.

Type: String

Valid Values: seconds | minutes | hours | days

Required: No

IdToken

A time unit for the value that you set in the `IdTokenValidity` parameter. The default `IdTokenValidity` time unit is hours. `IdTokenValidity` duration can range from five minutes to one day.

Type: String

Valid Values: seconds | minutes | hours | days

Required: No

RefreshToken

A time unit for the value that you set in the `RefreshTokenValidity` parameter. The default `RefreshTokenValidity` time unit is days. `RefreshTokenValidity` duration can range from 60 minutes to 10 years.

Type: String

Valid Values: seconds | minutes | hours | days

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](#)

UICustomizationType

A container for the UI customization information for the hosted UI in a user pool.

This data type is a response parameter of [DescribeUserPoolClient](#).

Contents

ClientId

The app client ID for your UI customization. When this value isn't present, the customization applies to all user pool app clients that don't have client-level settings..

Type: String

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

Pattern: `[\w+]+`

Required: No

CreationDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

CSS

The CSS values in the UI customization.

To get a template with your UI customization options, make a [GetUICustomization](#) request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

CSSVersion

The CSS version number.

Type: String

Required: No

ImageUrl

A URL path to the hosted logo image of your UI customization.

Type: String

Required: No

LastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

UserPoolId

The ID of the user pool with hosted UI customizations.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#)

UserAttributeUpdateSettingsType

The settings for updates to user attributes. These settings include the property `AttributesRequireVerificationBeforeUpdate`, a user-pool setting that tells Amazon Cognito how to handle changes to the value of your users' email address and phone number attributes. For more information, see [Verifying updates to email addresses and phone numbers](#).

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

AttributesRequireVerificationBeforeUpdate

Requires that your user verifies their email address, phone number, or both before Amazon Cognito updates the value of that attribute. When you update a user attribute that has this option activated, Amazon Cognito sends a verification message to the new phone number or email address. Amazon Cognito doesn't change the value of the attribute until your user responds to the verification message and confirms the new value.

You can verify an updated email address or phone number with a [VerifyUserAttribute](#) API request. You can also call the [AdminUpdateUserAttributes](#) API and set `email_verified` or `phone_number_verified` to true.

When `AttributesRequireVerificationBeforeUpdate` is false, your user pool doesn't require that your users verify attribute changes before Amazon Cognito updates them. In a user pool where `AttributesRequireVerificationBeforeUpdate` is false, API operations that change attribute values can immediately update a user's email or phone_number attribute.

Type: Array of strings

Valid Values: `phone_number` | `email`

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](#)

UserContextDataType

Contextual data, such as the user's device fingerprint, IP address, or location, used for evaluating the risk of an unexpected event by Amazon Cognito threat protection.

This data type is a request parameter of public-client authentication operations like [InitiateAuth](#) and [RespondToAuthChallenge](#).

Contents

EncodedData

Encoded device-fingerprint details that your app collected with the Amazon Cognito context data collection library. For more information, see [Adding user device and session data to API requests](#).

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

IpAddress

The source IP address of your user's device.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

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](#)

UserImportJobType

A user import job in a user pool. Describes the status of user import with a CSV file. For more information, see [Importing users into user pools from a CSV file](#).

This data type is a request parameter of [CreateUserImportJob](#), [DescribeUserImportJob](#), [ListUserImportJobs](#), [StartUserImportJob](#), and [StopUserImportJob](#).

Contents

CloudWatchLogsRoleArn

The role Amazon Resource Name (ARN) for the Amazon CloudWatch Logging role for the user import job. For more information, see "Creating the CloudWatch Logs IAM Role" in the Amazon Cognito Developer Guide.

Type: String

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

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

Required: No

CompletionDate

The date when the user import job was completed.

Type: Timestamp

Required: No

CompletionMessage

The message returned when the user import job is completed.

Type: String

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

Pattern: `[\w]+`

Required: No

CreationDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

FailedUsers

The number of users that couldn't be imported.

Type: Long

Required: No

ImportedUsers

The number of users that were successfully imported.

Type: Long

Required: No

JobId

The ID of the user import job.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `import-[0-9a-zA-Z-]+`

Required: No

JobName

The friendly name of the user import job.

Type: String

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

Pattern: `[\w\s+=, .@- ]+`

Required: No

PreSignedUrl

The pre-signed URL target for uploading the CSV file.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

Required: No

SkippedUsers

The number of users that were skipped.

Type: Long

Required: No

StartDate

The date when the user import job was started.

Type: Timestamp

Required: No

Status

The status of the user import job. One of the following:

- **Created** - The job was created but not started.
- **Pending** - A transition state. You have started the job, but it has not begun importing users yet.
- **InProgress** - The job has started, and users are being imported.
- **Stopping** - You have stopped the job, but the job has not stopped importing users yet.
- **Stopped** - You have stopped the job, and the job has stopped importing users.
- **Succeeded** - The job has completed successfully.
- **Failed** - The job has stopped due to an error.
- **Expired** - You created a job, but did not start the job within 24-48 hours. All data associated with the job was deleted, and the job can't be started.

Type: String

Valid Values: Created | Pending | InProgress | Stopping | Expired | Stopped
| Failed | Succeeded

Required: No

UserPoolId

The ID of the user pool that the users are being imported into.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

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](#)

UsernameConfigurationType

The configuration of a user pool for username case sensitivity.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

CaseSensitive

Specifies whether user name case sensitivity will be applied for all users in the user pool through Amazon Cognito APIs. For most use cases, set case sensitivity to `False` (case insensitive) as a best practice. When usernames and email addresses are case insensitive, users can sign in as the same user when they enter a different capitalization of their user name.

Valid values include:

`true`

Enables case sensitivity for all username input. When this option is set to `true`, users must sign in using the exact capitalization of their given username, such as "UserName". This is the default value.

`false`

Enables case insensitivity for all username input. For example, when this option is set to `false`, users can sign in using `username`, `USERNAME`, or `UserName`. This option also enables both `preferred_username` and `email` alias to be case insensitive, in addition to the `username` attribute.

Type: Boolean

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](#)

UserPoolAddOnsType

Contains settings for activation of threat protection, including the operating mode and additional authentication types. To log user security information but take no action, set to AUDIT. To configure automatic security responses to potentially unwanted traffic to your user pool, set to ENFORCED.

For more information, see [Adding advanced security to a user pool](#). To activate this setting, your user pool must be on the [Plus tier](#).

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

AdvancedSecurityMode

The operating mode of threat protection for standard authentication types in your user pool, including username-password and secure remote password (SRP) authentication.

Type: String

Valid Values: OFF | AUDIT | ENFORCED

Required: Yes

AdvancedSecurityAdditionalFlows

Threat protection configuration options for additional authentication types in your user pool, including custom authentication.

Type: [AdvancedSecurityAdditionalFlowsType](#) 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](#)

UserPoolClientDescription

A short description of a user pool app client.

This data type is a response parameter of [ListUserPoolClients](#).

Contents

ClientId

The app client ID.

Type: String

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

Pattern: `[\w+]`

Required: No

ClientName

The app client name.

Type: String

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

Pattern: `[\w\s+=, .@-]`

Required: No

UserPoolId

The ID of the user pool that's associated with the app client.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]`

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](#)

UserPoolClientType

The configuration of a user pool client.

This data type is a request parameter of [CreateUserPoolClient](#) and [UpdateUserPoolClient](#), and a response parameter of [DescribeUserPoolClient](#).

Contents

AccessTokenValidity

The access token time limit. After this limit expires, your user can't use their access token. To specify the time unit for `AccessTokenValidity` as seconds, minutes, hours, or days, set a `TokenValidityUnits` value in your API request.

For example, when you set `AccessTokenValidity` to 10 and `TokenValidityUnits` to hours, your user can authorize access with their access token for 10 hours.

The default time unit for `AccessTokenValidity` in an API request is hours. *Valid range* is displayed below in seconds.

If you don't specify otherwise in the configuration of your app client, your access tokens are valid for one hour.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 86400.

Required: No

AllowedOAuthFlows

The OAuth grant types that you want your app client to generate. To create an app client that generates client credentials grants, you must add `client_credentials` as the only allowed OAuth flow.

code

Use a code grant flow, which provides an authorization code as the response. This code can be exchanged for access tokens with the `/oauth2/token` endpoint.

implicit

Issue the access token (and, optionally, ID token, based on scopes) directly to your user.

`client_credentials`

Issue the access token from the `/oauth2/token` endpoint directly to a non-person user using a combination of the client ID and client secret.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 3 items.

Valid Values: `code` | `implicit` | `client_credentials`

Required: No

AllowedOAuthFlowsUserPoolClient

Set to `true` to use OAuth 2.0 authorization server features in your app client.

This parameter must have a value of `true` before you can configure the following features in your app client.

- `CallbackURLs`: Callback URLs.
- `LogoutURLs`: Sign-out redirect URLs.
- `AllowedOAuthScopes`: OAuth 2.0 scopes.
- `AllowedOAuthFlows`: Support for authorization code, implicit, and client credentials OAuth 2.0 grants.

To use authorization server features, configure one of these features in the Amazon Cognito console or set `AllowedOAuthFlowsUserPoolClient` to `true` in a `CreateUserPoolClient` or `UpdateUserPoolClient` API request. If you don't set a value for `AllowedOAuthFlowsUserPoolClient` in a request with the AWS CLI or SDKs, it defaults to `false`. When `false`, only SDK-based API sign-in is permitted.

Type: Boolean

Required: No

AllowedOAuthScopes

The OAuth 2.0 scopes that you want your app client to support. Can include standard OAuth scopes like `phone`, `email`, `openid`, and `profile`. Can also include the `aws.cognito.signin.user.admin` scope that authorizes user profile self-service operations and custom scopes from resource servers.

Type: Array of strings

Array Members: Maximum number of 50 items.

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

Pattern: `[\x21\x23-\x5B\x5D-\x7E]+`

Required: No

AnalyticsConfiguration

The user pool analytics configuration for collecting metrics and sending them to your Amazon Pinpoint campaign.

Note

In AWS Regions where Amazon Pinpoint isn't available, user pools only support sending events to Amazon Pinpoint projects in AWS Region us-east-1. In Regions where Amazon Pinpoint is available, user pools support sending events to Amazon Pinpoint projects within that same Region.

Type: [AnalyticsConfigurationType](#) object

Required: No

AuthSessionValidity

Amazon Cognito creates a session token for each API request in an authentication flow. `AuthSessionValidity` is the duration, in minutes, of that session token. Your user pool native user must respond to each authentication challenge before the session expires.

Type: Integer

Valid Range: Minimum value of 3. Maximum value of 15.

Required: No

CallbackURLs

A list of allowed redirect (callback) URLs for the IdPs.

A redirect URI must:

- Be an absolute URI.
- Be registered with the authorization server.
- Not include a fragment component.

See [OAuth 2.0 - Redirection Endpoint](#).

Amazon Cognito requires HTTPS over HTTP for callback URLs to `http://localhost`, `http://127.0.0.1` and `http://[::1]`. These callback URLs are for testing purposes only. You can specify custom TCP ports for your callback URLs.

App callback URLs such as `myapp://example` are also supported.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: No

ClientId

The ID of the app client.

Type: String

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

Pattern: `[\w+]`

Required: No

ClientName

The name of the app client.

Type: String

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

Pattern: `[\w\s+=, .@-]`

Required: No

ClientSecret

The app client secret.

Type: String

Length Constraints: Minimum length of 24. Maximum length of 64.

Pattern: `[\w+]+`

Required: No

CreationDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

DefaultRedirectURI

The default redirect URI. Must be in the `CallbackURLs` list.

A redirect URI must:

- Be an absolute URI.
- Be registered with the authorization server.
- Not include a fragment component.

See [OAuth 2.0 - Redirection Endpoint](#).

Amazon Cognito requires HTTPS over HTTP for callback URLs to `http://localhost`, `http://127.0.0.1` and `http://[::1]`. These callback URLs are for testing purposes only. You can specify custom TCP ports for your callback URLs.

App callback URLs such as `myapp://example` are also supported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: No

EnablePropagateAdditionalUserContextData

When `EnablePropagateAdditionalUserContextData` is true, Amazon Cognito accepts an `IpAddress` value that you send in the `UserContextData` parameter. The `UserContextData` parameter sends information to Amazon Cognito threat protection for risk analysis. You can send `UserContextData` when you sign in Amazon Cognito native users with the `InitiateAuth` and `RespondToAuthChallenge` API operations.

When `EnablePropagateAdditionalUserContextData` is false, you can't send your user's source IP address to Amazon Cognito threat protection with unauthenticated API operations. `EnablePropagateAdditionalUserContextData` doesn't affect whether you can send a source IP address in a `ContextData` parameter with the authenticated API operations `AdminInitiateAuth` and `AdminRespondToAuthChallenge`.

You can only activate `EnablePropagateAdditionalUserContextData` in an app client that has a client secret. For more information about propagation of user context data, see [Adding user device and session data to API requests](#).

Type: Boolean

Required: No

EnableTokenRevocation

Indicates whether token revocation is activated for the user pool client. When you create a new user pool client, token revocation is activated by default.

For more information about revoking tokens, see [RevokeToken](#).

Type: Boolean

Required: No

ExplicitAuthFlows

The [authentication flows](#) that you want your user pool client to support. For each app client in your user pool, you can sign in your users with any combination of one or more flows, including with a user name and Secure Remote Password (SRP), a user name and password, or a custom authentication process that you define with Lambda functions.

Note

If you don't specify a value for `ExplicitAuthFlows`, your app client supports `ALLOW_REFRESH_TOKEN_AUTH`, `ALLOW_USER_SRP_AUTH`, and `ALLOW_CUSTOM_AUTH`.

The values for authentication flow options include the following.

- `ALLOW_USER_AUTH`: Enable selection-based sign-in with `USER_AUTH`. This setting covers username-password, secure remote password (SRP), passwordless, and passkey authentication. This authentication flow can do username-password and SRP authentication without other `ExplicitAuthFlows` permitting them. For example users can complete an SRP challenge through `USER_AUTH` without the flow `USER_SRP_AUTH` being active for the app client. This flow doesn't include `CUSTOM_AUTH`.

To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

- `ALLOW_ADMIN_USER_PASSWORD_AUTH`: Enable admin based user password authentication flow `ADMIN_USER_PASSWORD_AUTH`. This setting replaces the `ADMIN_NO_SRP_AUTH` setting. With this authentication flow, your app passes a user name and password to Amazon Cognito in the request, instead of using the Secure Remote Password (SRP) protocol to securely transmit the password.
- `ALLOW_CUSTOM_AUTH`: Enable Lambda trigger based authentication.
- `ALLOW_USER_PASSWORD_AUTH`: Enable user password-based authentication. In this flow, Amazon Cognito receives the password in the request instead of using the SRP protocol to verify passwords.
- `ALLOW_USER_SRP_AUTH`: Enable SRP-based authentication.
- `ALLOW_REFRESH_TOKEN_AUTH`: Enable authflow to refresh tokens.

In some environments, you will see the values `ADMIN_NO_SRP_AUTH`, `CUSTOM_AUTH_FLOW_ONLY`, or `USER_PASSWORD_AUTH`. You can't assign these legacy `ExplicitAuthFlows` values to user pool clients at the same time as values that begin with `ALLOW_`, like `ALLOW_USER_SRP_AUTH`.

Type: Array of strings

Valid Values: `ADMIN_NO_SRP_AUTH` | `CUSTOM_AUTH_FLOW_ONLY` | `USER_PASSWORD_AUTH` | `ALLOW_ADMIN_USER_PASSWORD_AUTH` |

ALLOW_CUSTOM_AUTH | ALLOW_USER_PASSWORD_AUTH | ALLOW_USER_SRP_AUTH |
ALLOW_REFRESH_TOKEN_AUTH | ALLOW_USER_AUTH

Required: No

IdTokenValidity

The ID token time limit. After this limit expires, your user can't use their ID token. To specify the time unit for IdTokenValidity as seconds, minutes, hours, or days, set a TokenValidityUnits value in your API request.

For example, when you set IdTokenValidity as 10 and TokenValidityUnits as hours, your user can authenticate their session with their ID token for 10 hours.

The default time unit for IdTokenValidity in an API request is hours. *Valid range* is displayed below in seconds.

If you don't specify otherwise in the configuration of your app client, your ID tokens are valid for one hour.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 86400.

Required: No

LastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

LogoutURLs

A list of allowed logout URLs for the IdPs.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: No

PreventUserExistenceErrors

When ENABLED, suppresses messages that might indicate a valid user exists when someone attempts sign-in. This parameters sets your preference for the errors and responses that you want Amazon Cognito APIs to return during authentication, account confirmation, and password recovery when the user doesn't exist in the user pool. When set to ENABLED and the user doesn't exist, authentication returns an error indicating either the username or password was incorrect. Account confirmation and password recovery return a response indicating a code was sent to a simulated destination. When set to LEGACY, those APIs return a `UserNotFoundException` exception if the user doesn't exist in the user pool.

Defaults to LEGACY.

This setting affects the behavior of the following API operations.

- [AdminInitiateAuth](#)
- [AdminRespondToAuthChallenge](#)
- [InitiateAuth](#)
- [RespondToAuthChallenge](#)
- [ForgotPassword](#)
- [ConfirmForgotPassword](#)
- [ConfirmSignUp](#)
- [ResendConfirmationCode](#)

Type: String

Valid Values: LEGACY | ENABLED

Required: No

ReadAttributes

The list of user attributes that you want your app client to have read access to. After your user authenticates in your app, their access token authorizes them to read their own attribute value for any attribute in this list.

An example of this kind of activity is when your user selects a link to view their profile information. Your app makes a [GetUser](#) API request to retrieve and display your user's profile data.

When you don't specify the `ReadAttributes` for your app client, your app can read the values of `email_verified`, `phone_number_verified`, and the standard attributes of your user pool. When your user pool app client has read access to these default attributes, `ReadAttributes` doesn't return any information. Amazon Cognito only populates `ReadAttributes` in the API response if you have specified your own custom set of read attributes.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

RefreshTokenRotation

The configuration of your app client for refresh token rotation. When enabled, your app client issues new ID, access, and refresh tokens when users renew their sessions with refresh tokens. When disabled, token refresh issues only ID and access tokens.

Refresh token rotation must be completed with [GetTokensFromRefreshToken](#). With refresh token rotation disabled, you can complete token refresh with `GetTokensFromRefreshToken` and with `REFRESH_TOKEN_AUTH` in [InitiateAuth:AuthFlow](#) and [AdminInitiateAuth:AuthFlow](#).

Type: [RefreshTokenRotationType](#) object

Required: No

RefreshTokenValidity

The refresh token time limit. After this limit expires, your user can't use their refresh token. To specify the time unit for `RefreshTokenValidity` as seconds, minutes, hours, or days, set a `TokenValidityUnits` value in your API request.

For example, when you set `RefreshTokenValidity` as 10 and `TokenValidityUnits` as days, your user can refresh their session and retrieve new access and ID tokens for 10 days.

The default time unit for `RefreshTokenValidity` in an API request is days. You can't set `RefreshTokenValidity` to 0. If you do, Amazon Cognito overrides the value with the default value of 30 days. *Valid range* is displayed below in seconds.

If you don't specify otherwise in the configuration of your app client, your refresh tokens are valid for 30 days.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 315360000.

Required: No

SupportedIdentityProviders

A list of provider names for the identity providers (IdPs) that are supported on this client. The following are supported: COGNITO, Facebook, Google, SignInWithApple, and LoginWithAmazon. You can also specify the names that you configured for the SAML and OIDC IdPs in your user pool, for example MySAMLIdP or MyOIDCIdP.

This parameter sets the IdPs that [managed login](#) will display on the login page for your app client. The removal of COGNITO from this list doesn't prevent authentication operations for local users with the user pools API in an AWS SDK. The only way to prevent SDK-based authentication is to block access with a [AWS WAF rule](#).

Type: Array of strings

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\p{Z}]`+

Required: No

TokenValidityUnits

The time units that, with `IdTokenValidity`, `AccessTokenValidity`, and `RefreshTokenValidity`, set and display the duration of ID, access, and refresh tokens for an app client. You can assign a separate token validity unit to each type of token.

Type: [TokenValidityUnitsType](#) object

Required: No

UserPoolId

The ID of the user pool associated with the app client.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: No

WriteAttributes

The list of user attributes that you want your app client to have write access to. After your user authenticates in your app, their access token authorizes them to set or modify their own attribute value for any attribute in this list.

An example of this kind of activity is when you present your user with a form to update their profile information and they change their last name. Your app then makes an [UpdateUserAttributes](#) API request and sets `family_name` to the new value.

When you don't specify the `WriteAttributes` for your app client, your app can write the values of the Standard attributes of your user pool. When your user pool has write access to these default attributes, `WriteAttributes` doesn't return any information. Amazon Cognito only populates `WriteAttributes` in the API response if you have specified your own custom set of write attributes.

If your app client allows users to sign in through an IdP, this array must include all attributes that you have mapped to IdP attributes. Amazon Cognito updates mapped attributes when users sign in to your application through an IdP. If your app client does not have write access to a mapped attribute, Amazon Cognito throws an error when it tries to update the attribute. For more information, see [Specifying IdP Attribute Mappings for Your user pool](#).

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 2048.

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](#)

UserPoolDescriptionType

A short description of a user pool.

This data type is a response parameter of [ListUserPools](#).

Contents

CreationDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

Id

The user pool ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+\_[0-9a-zA-Z]+`

Required: No

LambdaConfig

A collection of user pool Lambda triggers. Amazon Cognito invokes triggers at several possible stages of user pool operations. Triggers can modify the outcome of the operations that invoked them.

Type: [LambdaConfigType](#) object

Required: No

LastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

Name

The user pool name.

Type: String

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

Pattern: `[\w\s+=, .@- ]+`

Required: No

Status

This member has been deprecated.

The user pool status.

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](#)

UserPoolPolicyType

A list of user pool policies. Contains the policy that sets password-complexity requirements.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

PasswordPolicy

The password policy settings for a user pool, including complexity, history, and length requirements.

Type: [PasswordPolicyType](#) object

Required: No

SignInPolicy

The policy for allowed types of authentication in a user pool.

Type: [SignInPolicyType](#) 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](#)

UserPoolType

The configuration of a user pool.

This data type is a response parameter of [CreateUserPool](#), [UpdateUserPool](#), and [DescribeUserPool](#).

Contents

AccountRecoverySetting

The available verified method a user can use to recover their password when they call `ForgotPassword`. You can use this setting to define a preferred method when a user has more than one method available. With this setting, SMS doesn't qualify for a valid password recovery mechanism if the user also has SMS multi-factor authentication (MFA) activated. In the absence of this setting, Amazon Cognito uses the legacy behavior to determine the recovery method where SMS is preferred through email.

Type: [AccountRecoverySettingType](#) object

Required: No

AdminCreateUserConfig

The configuration for `AdminCreateUser` requests.

Type: [AdminCreateUserConfigType](#) object

Required: No

AliasAttributes

Attributes supported as an alias for this user pool. An alias is an attribute that users can enter as an alternative username. Possible values: **phone_number**, **email**, or **preferred_username**.

Type: Array of strings

Valid Values: `phone_number` | `email` | `preferred_username`

Required: No

Arn

The Amazon Resource Name (ARN) of the user pool.

Type: String

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

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

Required: No

AutoVerifiedAttributes

The attributes that are auto-verified in a user pool.

Type: Array of strings

Valid Values: `phone_number` | `email`

Required: No

CreationDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

CustomDomain

A custom domain name that you provide to Amazon Cognito. This parameter applies only if you use a custom domain to host the sign-up and sign-in pages for your application. An example of a custom domain name might be `auth.example.com`.

For more information about adding a custom domain to your user pool, see [Using Your Own Domain for the Hosted UI](#).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 63.

Pattern: `^[a-z0-9](?:[a-z0-9-]{0,61}[a-z0-9])?$`

Required: No

DeletionProtection

When active, DeletionProtection prevents accidental deletion of your user pool. Before you can delete a user pool that you have protected against deletion, you must deactivate this feature.

When you try to delete a protected user pool in a DeleteUserPool API request, Amazon Cognito returns an InvalidParameterException error. To delete a protected user pool, send a new DeleteUserPool request after you deactivate deletion protection in an UpdateUserPool API request.

Type: String

Valid Values: ACTIVE | INACTIVE

Required: No

DeviceConfiguration

The device-remembering configuration for a user pool. A null value indicates that you have deactivated device remembering in your user pool.

Note

When you provide a value for any DeviceConfiguration field, you activate the Amazon Cognito device-remembering feature.

Type: [DeviceConfigurationType](#) object

Required: No

Domain

The domain prefix, if the user pool has a domain associated with it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 63.

Pattern: `^[a-z0-9](?:[a-z0-9\-\]{0,61}[a-z0-9])?$`

Required: No

EmailConfiguration

The email configuration of your user pool. The email configuration type sets your preferred sending method, AWS Region, and sender for messages from your user pool.

Type: [EmailConfigurationType](#) object

Required: No

EmailConfigurationFailure

Deprecated. Review error codes from API requests with EventSource:cognito-idp.amazonaws.com in AWS CloudTrail for information about problems with user pool email configuration.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

EmailVerificationMessage

This parameter is no longer used. See [VerificationMessageTemplateType](#).

This parameter is no longer used.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 20000.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s*]*\{####\}`
`[\p{L}\p{M}\p{S}\p{N}\p{P}\s*]*`

Required: No

EmailVerificationSubject

This parameter is no longer used. See [VerificationMessageTemplateType](#).

This parameter is no longer used.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 140.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s]+`

Required: No

EstimatedNumberOfUsers

A number estimating the size of the user pool.

Type: Integer

Required: No

Id

The ID of the user pool.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 55.

Pattern: `[\w-]+_[0-9a-zA-Z]+`

Required: No

LambdaConfig

A collection of user pool Lambda triggers. Amazon Cognito invokes triggers at several possible stages of user pool operations. Triggers can modify the outcome of the operations that invoked them.

Type: [LambdaConfigType](#) object

Required: No

LastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

MfaConfiguration

Can be one of the following values:

- OFF - MFA tokens aren't required and can't be specified during user registration.
- ON - MFA tokens are required for all user registrations. You can only specify required when you're initially creating a user pool.
- OPTIONAL - Users have the option when registering to create an MFA token.

Type: String

Valid Values: OFF | ON | OPTIONAL

Required: No

Name

The name of the user pool.

Type: String

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

Pattern: `[\w\s+=, .@- ]+`

Required: No

Policies

A list of user pool policies. Contains the policy that sets password-complexity requirements.

Type: [UserPoolPolicyType](#) object

Required: No

SchemaAttributes

A list of the user attributes and their properties in your user pool. The attribute schema contains standard attributes, custom attributes with a `custom:` prefix, and developer attributes with a `dev:` prefix. For more information, see [User pool attributes](#).

Developer-only attributes are a legacy feature of user pools, and are read-only to all app clients. You can create and update developer-only attributes only with IAM-authenticated API operations. Use app client read/write permissions instead.

Type: Array of [SchemaAttributeType](#) objects

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

Required: No

SmsAuthenticationMessage

The contents of the SMS authentication message.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 140.

Pattern: `.*\{####\}.*`

Required: No

SmsConfiguration

User pool configuration for delivery of SMS messages with Amazon Simple Notification Service. To send SMS messages with Amazon SNS in the AWS Region that you want, the Amazon Cognito user pool uses an AWS Identity and Access Management (IAM) role in your AWS account.

Type: [SmsConfigurationType](#) object

Required: No

SmsConfigurationFailure

The reason why the SMS configuration can't send the messages to your users.

This message might include comma-separated values to describe why your SMS configuration can't send messages to user pool end users.

InvalidSmsRoleAccessPolicyException

The AWS Identity and Access Management role that Amazon Cognito uses to send SMS messages isn't properly configured. For more information, see [SmsConfigurationType](#).

SNSSandbox

The AWS account is in the SNS SMS Sandbox and messages will only reach verified end users. This parameter won't get populated with SNSSandbox if the user creating the user pool doesn't have SNS permissions. To learn how to move your AWS account out of the sandbox, see [Moving out of the SMS sandbox](#).

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: No

SmsVerificationMessage

This parameter is no longer used. See [VerificationMessageTemplateType](#).

This parameter is no longer used.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 140.

Pattern: `.*\{####\}.*`

Required: No

Status

This member has been deprecated.

This parameter is no longer used.

Type: String

Valid Values: Enabled | Disabled

Required: No

UserAttributeUpdateSettings

The settings for updates to user attributes. These settings include the property `AttributesRequireVerificationBeforeUpdate`, a user-pool setting that tells Amazon Cognito how to handle changes to the value of your users' email address and phone number attributes. For more information, see [Verifying updates to email addresses and phone numbers](#).

Type: [UserAttributeUpdateSettingsType](#) object

Required: No

UsernameAttributes

Specifies whether a user can use an email address or phone number as a username when they sign up.

Type: Array of strings

Valid Values: phone_number | email

Required: No

UsernameConfiguration

Case sensitivity of the username input for the selected sign-in option. When case sensitivity is set to `False` (case insensitive), users can sign in with any combination of capital and lowercase letters. For example, `username`, `USERNAME`, or `UserName`, or for email, `email@example.com` or `EMail@eXample.Com`. For most use cases, set case sensitivity to `False` (case insensitive) as a best practice. When usernames and email addresses are case insensitive, Amazon Cognito treats any variation in case as the same user, and prevents a case variation from being assigned to the same attribute for a different user.

This configuration is immutable after you set it. For more information, see [UsernameConfigurationType](#).

Type: [UsernameConfigurationType](#) object

Required: No

UserPoolAddOns

Contains settings for activation of threat protection, including the operating mode and additional authentication types. To log user security information but take no action, set to `AUDIT`. To configure automatic security responses to potentially unwanted traffic to your user pool, set to `ENFORCED`.

For more information, see [Adding advanced security to a user pool](#). To activate this setting, your user pool must be on the [Plus tier](#).

Type: [UserPoolAddOnsType](#) object

Required: No

UserPoolTags

The tags that are assigned to the user pool. A tag is a label that you can apply to user pools to categorize and manage them in different ways, such as by purpose, owner, environment, or other criteria.

Type: String to string map

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

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

Required: No

UserPoolTier

The user pool [feature plan](#), or tier. This parameter determines the eligibility of the user pool for features like managed login, access-token customization, and threat protection. Defaults to ESSENTIALS.

Type: String

Valid Values: LITE | ESSENTIALS | PLUS

Required: No

VerificationMessageTemplate

The template for the verification message that your user pool delivers to users who set an email address or phone number attribute.

Type: [VerificationMessageTemplateType](#) 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](#)

UserType

A user profile in a Amazon Cognito user pool.

This data type is a response parameter to [AdminCreateUser](#) and [ListUsers](#).

Contents

Attributes

Names and values of a user's attributes, for example email.

Type: Array of [AttributeType](#) objects

Required: No

Enabled

Indicates whether the user's account is enabled or disabled.

Type: Boolean

Required: No

MFAOptions

The user's MFA configuration.

Type: Array of [MFAOptionType](#) objects

Required: No

UserCreateDate

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

UserLastModifiedDate

The date and time when the item was modified. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: No

Username

The user's username.

Type: String

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

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}]+`

Required: No

UserStatus

The user status. This can be one of the following:

- UNCONFIRMED: User has been created but not confirmed.
- CONFIRMED: User has been confirmed.
- EXTERNAL_PROVIDER: User signed in with a third-party IdP.
- RESET_REQUIRED: User is confirmed, but the user must request a code and reset their password before they can sign in.
- FORCE_CHANGE_PASSWORD: The user is confirmed and the user can sign in using a temporary password, but on first sign-in, the user must change their password to a new value before doing anything else.

The statuses ARCHIVED, UNKNOWN, and COMPROMISED are no longer used.

Type: String

Valid Values: UNCONFIRMED | CONFIRMED | ARCHIVED | COMPROMISED | UNKNOWN | RESET_REQUIRED | FORCE_CHANGE_PASSWORD | EXTERNAL_PROVIDER

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](#)

VerificationMessageTemplateType

The template for the verification message that your user pool delivers to users who set an email address or phone number attribute.

This data type is a request and response parameter of [CreateUserPool](#) and [UpdateUserPool](#), and a response parameter of [DescribeUserPool](#).

Contents

DefaultEmailOption

The configuration of verification emails to contain a clickable link or a verification code.

For link, your template body must contain link text in the format {##Click here##}. "Click here" in the example is a customizable string. For code, your template body must contain a code placeholder in the format {####}.

Type: String

Valid Values: CONFIRM_WITH_LINK | CONFIRM_WITH_CODE

Required: No

EmailMessage

The template for email messages that Amazon Cognito sends to your users. You can set an EmailMessage template only if the value of [EmailSendingAccount](#) is DEVELOPER. When your [EmailSendingAccount](#) is DEVELOPER, your user pool sends email messages with your own Amazon SES configuration.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 20000.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s*]*\{####\}`
`[\p{L}\p{M}\p{S}\p{N}\p{P}\s*]*`

Required: No

EmailMessageByLink

The email message template for sending a confirmation link to the user. You can set an EmailMessageByLink template only if the value of [EmailSendingAccount](#) is DEVELOPER.

When your [EmailSendingAccount](#) is DEVELOPER, your user pool sends email messages with your own Amazon SES configuration.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 20000.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s]*`
`\{##[\p{L}\p{M}\p{S}\p{N}\p{P}\s]*##\}[\p{L}\p{M}\p{S}\p{N}\p{P}\s]*`

Required: No

EmailSubject

The subject line for the email message template. You can set an EmailSubject template only if the value of [EmailSendingAccount](#) is DEVELOPER. When your [EmailSendingAccount](#) is DEVELOPER, your user pool sends email messages with your own Amazon SES configuration.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 140.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s]+`

Required: No

EmailSubjectByLink

The subject line for the email message template for sending a confirmation link to the user. You can set an EmailSubjectByLink template only if the value of [EmailSendingAccount](#) is DEVELOPER. When your [EmailSendingAccount](#) is DEVELOPER, your user pool sends email messages with your own Amazon SES configuration.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 140.

Pattern: `[\p{L}\p{M}\p{S}\p{N}\p{P}\s]+`

Required: No

SmsMessage

The template for SMS messages that Amazon Cognito sends to your users.

Type: String

Length Constraints: Minimum length of 6. Maximum length of 140.

Pattern: `.*\{####\}.*`

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](#)

WebAuthnConfigurationType

Settings for authentication (MFA) with passkey, or webauthN, biometric and security-key devices in a user pool. Configures the following:

- Configuration for requiring user-verification support in passkeys.
- The user pool relying-party ID. This is the domain, typically your user pool domain, that user's passkey providers should trust as a receiver of passkey authentication.
- The providers that you want to allow as origins for passkey authentication.

This data type is a request parameter of [SetUserPoolMfaConfig](#) and a response parameter of [GetUserPoolMfaConfig](#). To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

Contents

FactorConfiguration

Sets whether passkeys can be used as multi-factor authentication (MFA). When set to `MULTI_FACTOR_WITH_USER_VERIFICATION`, passkey authentication with user verification satisfies MFA requirements. When set to `SINGLE_FACTOR` or not set, passkeys are a single authentication factor. To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

Type: String

Valid Values: `SINGLE_FACTOR` | `MULTI_FACTOR_WITH_USER_VERIFICATION`

Required: No

RelyingPartyId

Sets or displays the authentication domain, typically your user pool domain, that passkey providers must use as a relying party (RP) in their configuration.

Under the following conditions, the passkey relying party ID must be the fully-qualified domain name of your custom domain:

- The user pool is configured for passkey authentication.
- The user pool has a custom domain, whether or not it also has a prefix domain.

- Your application performs authentication with managed login or the classic hosted UI.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 127.

Required: No

UserVerification

When required, users can only register and sign in users with passkeys that are capable of [user verification](#). When preferred, your user pool doesn't require the use of authenticators with user verification but encourages it.

Type: String

Valid Values: `required` | `preferred`

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](#)

WebAuthnCredentialDescription

The details of a passkey, or webauthN, biometric or security-key authentication factor for a user.

This data type is a response parameter of [ListWebAuthnCredentials](#). To activate this setting, your user pool must be in the [Essentials tier](#) or higher.

Contents

AuthenticatorTransports

Information about the transport methods of the passkey credential, for example USB or Bluetooth Low Energy.

Type: Array of strings

Required: Yes

CreatedAt

The date and time when the item was created. Amazon Cognito returns this timestamp in UNIX epoch time format. Your SDK might render the output in a human-readable format like ISO 8601 or a Java Date object.

Type: Timestamp

Required: Yes

CredentialId

The unique identifier of the passkey credential.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: Yes

FriendlyCredentialName

An automatically-generated friendly name for the passkey credential.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: Yes

RelyingPartyId

The relying-party ID of the provider for the passkey credential.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 131072.

Required: Yes

AuthenticatorAttachment

The general category of the passkey authenticator. Can be a platform, or on-device authenticator like a built-in fingerprint scanner, or a cross-platform device that's not attached to the device like a Bluetooth security key.

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](#)

WebAuthnMfaSettingsType

A user's preference for using passkey, or WebAuthn, multi-factor authentication (MFA). Turns passkey MFA on and off for the user. Unlike other MFA settings types, this type doesn't include a `PreferredMfa` option because passkey MFA applies only when passkey is the first authentication factor.

This data type is a request parameter of [SetUserMFAPreference](#) and [AdminSetUserMFAPreference](#).

Contents

Enabled

Specifies whether passkey MFA is activated for a user. When activated, the user's passkey authentication requires user verification, and passkey sign-in is available when MFA is required. The user must also have at least one other MFA method such as SMS, TOTP, or email activated to prevent account lockout.

Type: Boolean

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