Welcome

AWS Private CA Connector for SCEP

API Version 2018-05-10

AWS Private CA Connector for SCEP: Welcome

Table of Contents

Welcome

Connector for SCEP creates a connector between AWS Private CA and your SCEP-enabled clients and devices. For more information, see Connector for SCEP in the *AWS Private CA User Guide*.

This document was last published on January 27, 2026.

Actions

The following actions are supported:

- CreateChallenge
- CreateConnector
- DeleteChallenge
- DeleteConnector
- GetChallengeMetadata
- GetChallengePassword
- GetConnector
- ListChallengeMetadata
- ListConnectors
- ListTagsForResource
- TagResource
- UntagResource

CreateChallenge

For general-purpose connectors. Creates a *challenge password* for the specified connector. The SCEP protocol uses a challenge password to authenticate a request before issuing a certificate from a certificate authority (CA). Your SCEP clients include the challenge password as part of their certificate request to Connector for SCEP. To retrieve the connector Amazon Resource Names (ARNs) for the connectors in your account, call ListConnectors.

To create additional challenge passwords for the connector, call `CreateChallenge` again. We recommend frequently rotating your challenge passwords.

Request Syntax

```
POST /challenges HTTP/1.1
Content-type: application/json

{
   "ClientToken": "string",
   "ConnectorArn": "string",
   "Tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

ClientToken

Custom string that can be used to distinguish between calls to the CreateChallenge action. Client tokens for `CreateChallenge` time out after five minutes. Therefore, if you call `CreateChallenge` multiple times with the same client token within five minutes, Connector for SCEP recognizes that you are requesting only one challenge and will only respond with one. If you change the client token for each call, Connector for SCEP recognizes that you are requesting multiple challenge passwords.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[!-~]+`

Required: No

ConnectorArn

The Amazon Resource Name (ARN) of the connector that you want to create a challenge for.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Tags

The key-value pairs to associate with the resource.

Type: String to string map

Required: No

Response Syntax

```
HTTP/1.1 202
Content-type: application/json

{
   "Challenge": {
      "Arn": "string",
      "ConnectorArn": "string",
      "CreatedAt": number,
      "Password": "string",
      "UpdatedAt": number
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 202 response.

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

Challenge

Returns the challenge details for the specified connector.

Type: Challenge object

Errors

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

AccessDeniedException

You can receive this error if you attempt to perform an operation and you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

This request can't be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 409

InternalServerException

The request processing has failed because of an unknown error, exception or failure with an internal server.

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might be incorrectly specified, or it might have a status other than `ACTIVE`.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 404

ServiceQuotaExceededException

The request would cause a service quota to be exceeded.

QuotaCode

The quota identifier.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

ServiceCode

Identifies the originating service.

HTTP Status Code: 402

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a name tag, or an invalid pagination token.

Reason

The reason for the validation error, if available. The service doesn't return a reason for every validation 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
- 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

CreateConnector

Creates a SCEP connector. A SCEP connector links AWS Private Certificate Authority to your SCEP-compatible devices and mobile device management (MDM) systems. Before you create a connector, you must complete a set of prerequisites, including creation of a private certificate authority (CA) to use with this connector. For more information, see Connector for SCEP prerequisites.

Request Syntax

```
POST /connectors HTTP/1.1
Content-type: application/json

{
   "CertificateAuthorityArn": "string",
   "ClientToken": "string",
   "MobileDeviceManagement": { ... },
   "Tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

CertificateAuthorityArn

The Amazon Resource Name (ARN) of the AWS Private Certificate Authority certificate authority to use with this connector. Due to security vulnerabilities present in the SCEP protocol, we recommend using a private CA that's dedicated for use with the connector.

To retrieve the private CAs associated with your account, you can call ListCertificateAuthorities using the AWS Private CA API.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:acm-pca:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:certificate-authority\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

ClientToken

Custom string that can be used to distinguish between calls to the CreateChallenge action. Client tokens for `CreateChallenge` time out after five minutes. Therefore, if you call `CreateChallenge` multiple times with the same client token within five minutes, Connector for SCEP recognizes that you are requesting only one challenge and will only respond with one. If you change the client token for each call, Connector for SCEP recognizes that you are requesting multiple challenge passwords.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[!-~]+`

Required: No

MobileDeviceManagement

If you don't supply a value, by default Connector for SCEP creates a connector for general-purpose use. A general-purpose connector is designed to work with clients or endpoints that support the SCEP protocol, except Connector for SCEP for Microsoft Intune. With connectors for general-purpose use, you manage SCEP challenge passwords using Connector for SCEP. For information about considerations and limitations with using Connector for SCEP, see Considerations and Limitations.

If you provide an `IntuneConfiguration`, Connector for SCEP creates a connector for use with Microsoft Intune, and you manage the challenge passwords using Microsoft Intune. For more information, see Using Connector for SCEP for Microsoft Intune.

Type: MobileDeviceManagement object

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

Required: No

Tags

The key-value pairs to associate with the resource.

Type: String to string map

Required: No

Response Syntax

```
HTTP/1.1 202
Content-type: application/json

{
   "ConnectorArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 202 response.

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

ConnectorArn

Returns the Amazon Resource Name (ARN) of the connector.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Errors

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

AccessDeniedException

You can receive this error if you attempt to perform an operation and you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request can't be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 409

InternalServerException

The request processing has failed because of an unknown error, exception or failure with an internal server.

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might be incorrectly specified, or it might have a status other than `ACTIVE`.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 404

ServiceQuotaExceededException

The request would cause a service quota to be exceeded.

QuotaCode

The quota identifier.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

ServiceCode

Identifies the originating service.

HTTP Status Code: 402

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a name tag, or an invalid pagination token.

Reason

The reason for the validation error, if available. The service doesn't return a reason for every validation 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
- 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

DeleteChallenge

Deletes the specified Challenge.

Request Syntax

```
DELETE /challenges/ChallengeArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ChallengeArn

The Amazon Resource Name (ARN) of the challenge password to delete.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/challenge\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 202
```

Response Elements

If the action is successful, the service sends back an HTTP 202 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to perform an operation and you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request can't be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 409

InternalServerException

The request processing has failed because of an unknown error, exception or failure with an internal server.

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might be incorrectly specified, or it might have a status other than `ACTIVE`.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a name tag, or an invalid pagination token.

Reason

The reason for the validation error, if available. The service doesn't return a reason for every validation 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
- 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

DeleteConnector

Deletes the specified Connector. This operation also deletes any challenges associated with the connector.

Request Syntax

```
DELETE /connectors/ConnectorArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ConnectorArn

The Amazon Resource Name (ARN) of the connector to delete.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 202
```

Response Elements

If the action is successful, the service sends back an HTTP 202 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to perform an operation and you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request can't be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 409

InternalServerException

The request processing has failed because of an unknown error, exception or failure with an internal server.

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might be incorrectly specified, or it might have a status other than `ACTIVE`.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a name tag, or an invalid pagination token.

Reason

The reason for the validation error, if available. The service doesn't return a reason for every validation 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
- 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

GetChallengeMetadata

Retrieves the metadata for the specified Challenge.

Request Syntax

```
GET /challengeMetadata/ChallengeArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ChallengeArn

The Amazon Resource Name (ARN) of the challenge.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/challenge\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ChallengeMetadata": {
      "Arn": "string",
      "ConnectorArn": "string",
      "CreatedAt": number,
      "UpdatedAt": 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.

ChallengeMetadata

The metadata for the challenge.

Type: ChallengeMetadata object

Errors

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

AccessDeniedException

You can receive this error if you attempt to perform an operation and you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

The request processing has failed because of an unknown error, exception or failure with an internal server.

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might be incorrectly specified, or it might have a status other than `ACTIVE`.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a name tag, or an invalid pagination token.

Reason

The reason for the validation error, if available. The service doesn't return a reason for every validation 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
- 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

GetChallengePassword

Retrieves the challenge password for the specified Challenge.

Request Syntax

```
GET /challengePasswords/ChallengeArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ChallengeArn

The Amazon Resource Name (ARN) of the challenge.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/challenge\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "Password": "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.

Password

The SCEP challenge password.

Type: String

Errors

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

AccessDeniedException

You can receive this error if you attempt to perform an operation and you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

The request processing has failed because of an unknown error, exception or failure with an internal server.

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might be incorrectly specified, or it might have a status other than `ACTIVE`.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a name tag, or an invalid pagination token.

Reason

The reason for the validation error, if available. The service doesn't return a reason for every validation 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
- 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

GetConnector

Retrieves details about the specified Connector. Calling this action returns important details about the connector, such as the public SCEP URL where your clients can request certificates.

Request Syntax

```
GET /connectors/ConnectorArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ConnectorArn

The Amazon Resource Name (ARN) of the connector.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "Connector": {
      "Arn": "string",
      "CertificateAuthorityArn": "string",
      "CreatedAt": number,
      "Endpoint": "string",
```

```
      "MobileDeviceManagement": { ... },
      "OpenIdConfiguration": {
         "Audience": "string",
         "Issuer": "string",
         "Subject": "string"
      },
      "Status": "string",
      "StatusReason": "string",
      "Type": "string",
      "UpdatedAt": 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.

Connector

The properties of the connector.

Type: Connector object

Errors

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

AccessDeniedException

You can receive this error if you attempt to perform an operation and you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

The request processing has failed because of an unknown error, exception or failure with an internal server.

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might be incorrectly specified, or it might have a status other than `ACTIVE`.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a name tag, or an invalid pagination token.

Reason

The reason for the validation error, if available. The service doesn't return a reason for every validation 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
- 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

ListChallengeMetadata

Retrieves the challenge metadata for the specified ARN.

Request Syntax

```
GET /challengeMetadata?
ConnectorArn=ConnectorArn&MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ConnectorArn

The Amazon Resource Name (ARN) of the connector.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

MaxResults

The maximum number of objects that you want Connector for SCEP to return for this request. If more objects are available, in the response, Connector for SCEP provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

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

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Connector for SCEP returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Length Constraints: Minimum length of 1. Maximum length of 1000.

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "Challenges": [
      {
         "Arn": "string",
         "ConnectorArn": "string",
         "CreatedAt": number,
         "UpdatedAt": number
      }
   ],
   "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.

Challenges

The challenge metadata for the challenges belonging to your AWS account.

Type: Array of ChallengeMetadataSummary objects

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Connector for SCEP returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1000.

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

Errors

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

AccessDeniedException

You can receive this error if you attempt to perform an operation and you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

The request processing has failed because of an unknown error, exception or failure with an internal server.

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might be incorrectly specified, or it might have a status other than `ACTIVE`.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a name tag, or an invalid pagination token.

Reason

The reason for the validation error, if available. The service doesn't return a reason for every validation 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
- 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

ListConnectors

Lists the connectors belonging to your AWS account.

Request Syntax

```
GET /connectors?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults

The maximum number of objects that you want Connector for SCEP to return for this request. If more objects are available, in the response, Connector for SCEP provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

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

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Connector for SCEP returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Length Constraints: Minimum length of 1. Maximum length of 1000.

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "Connectors": [
      {
         "Arn": "string",
         "CertificateAuthorityArn": "string",
         "CreatedAt": number,
         "Endpoint": "string",
         "MobileDeviceManagement": { ... },
         "OpenIdConfiguration": {
            "Audience": "string",
            "Issuer": "string",
            "Subject": "string"
         },
         "Status": "string",
         "StatusReason": "string",
         "Type": "string",
         "UpdatedAt": number
      }
   ],
   "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.

Connectors

The connectors belonging to your AWS account.

Type: Array of ConnectorSummary objects

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Connector for SCEP returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1000.

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

Errors

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

AccessDeniedException

You can receive this error if you attempt to perform an operation and you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

The request processing has failed because of an unknown error, exception or failure with an internal server.

HTTP Status Code: 500

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a name tag, or an invalid pagination token.

Reason

The reason for the validation error, if available. The service doesn't return a reason for every validation 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
- 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

Retrieves the tags associated with the specified resource. Tags are key-value pairs that you can use to categorize and manage your resources, for purposes like billing. For example, you might set the tag key to "customer" and the value to the customer name or ID. You can specify one or more tags to add to each AWS resource, up to 50 tags for a resource.

Request Syntax

```
GET /tags/ResourceArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ResourceArn

The Amazon Resource Name (ARN) of the resource.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "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 key-value pairs to associate with the resource.

Type: String to string map

Errors

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

AccessDeniedException

You can receive this error if you attempt to perform an operation and you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

The request processing has failed because of an unknown error, exception or failure with an internal server.

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might be incorrectly specified, or it might have a status other than `ACTIVE`.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a name tag, or an invalid pagination token.

Reason

The reason for the validation error, if available. The service doesn't return a reason for every validation 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
- 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

Adds one or more tags to your resource.

Request Syntax

```
POST /tags/ResourceArn HTTP/1.1
Content-type: application/json

{
   "Tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

ResourceArn

The Amazon Resource Name (ARN) of the resource.

Required: Yes

Request Body

The request accepts the following data in JSON format.

Tags

The key-value pairs to associate with the resource.

Type: String to string map

Required: Yes

Response Syntax

```
HTTP/1.1 204
```

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to perform an operation and you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

The request processing has failed because of an unknown error, exception or failure with an internal server.

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might be incorrectly specified, or it might have a status other than `ACTIVE`.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a name tag, or an invalid pagination token.

Reason

The reason for the validation error, if available. The service doesn't return a reason for every validation 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
- 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

Removes one or more tags from your resource.

Request Syntax

```
DELETE /tags/ResourceArn?tagKeys=TagKeys HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ResourceArn

The Amazon Resource Name (ARN) of the resource.

Required: Yes

TagKeys

Specifies a list of tag keys that you want to remove from the specified resources.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 204
```

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to perform an operation and you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

The request processing has failed because of an unknown error, exception or failure with an internal server.

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might be incorrectly specified, or it might have a status other than `ACTIVE`.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be either `Connector` or `Challenge`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a name tag, or an invalid pagination token.

Reason

The reason for the validation error, if available. The service doesn't return a reason for every validation 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
- 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 Private CA Connector for SCEP 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:

- Challenge
- ChallengeMetadata
- ChallengeMetadataSummary
- Connector
- ConnectorSummary
- IntuneConfiguration
- MobileDeviceManagement
- OpenIdConfiguration

Challenge

For Connector for SCEP for general-purpose. An object containing information about the specified connector's SCEP challenge passwords.

Contents

Arn

The Amazon Resource Name (ARN) of the challenge.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/challenge\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

ConnectorArn

The Amazon Resource Name (ARN) of the connector.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CreatedAt

The date and time that the challenge was created.

Type: Timestamp

Required: No

Password

The SCEP challenge password, in UUID format.

Type: String

Required: No

UpdatedAt

The date and time that the challenge was updated.

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

ChallengeMetadata

Contains details about the connector's challenge.

Contents

Arn

The Amazon Resource Name (ARN) of the challenge.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/challenge\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

ConnectorArn

The Amazon Resource Name (ARN) of the connector.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CreatedAt

The date and time that the connector was created.

Type: Timestamp

Required: No

UpdatedAt

The date and time that the connector was updated.

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

ChallengeMetadataSummary

Details about the specified challenge, returned by the GetChallengeMetadata action.

Contents

Arn

The Amazon Resource Name (ARN) of the challenge.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/challenge\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

ConnectorArn

The Amazon Resource Name (ARN) of the connector.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CreatedAt

The date and time that the challenge was created.

Type: Timestamp

Required: No

UpdatedAt

The date and time that the challenge was updated.

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

Connector

Connector for SCEP is a service that links AWS Private Certificate Authority to your SCEP-enabled devices. The connector brokers the exchange of certificates from AWS Private CA to your SCEP-enabled devices and mobile device management systems. The connector is a complex type that contains the connector's configuration settings.

Contents

Arn

The Amazon Resource Name (ARN) of the connector.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CertificateAuthorityArn

The Amazon Resource Name (ARN) of the certificate authority associated with the connector.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:acm-pca:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:certificate-authority\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CreatedAt

The date and time that the connector was created.

Type: Timestamp

Required: No

Endpoint

The connector's HTTPS public SCEP URL.

Type: String

Required: No

MobileDeviceManagement

Contains settings relevant to the mobile device management system that you chose for the connector. If you didn't configure `MobileDeviceManagement`, then the connector is for general-purpose use and this object is empty.

Type: MobileDeviceManagement object

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

Required: No

OpenIdConfiguration

Contains OpenID Connect (OIDC) parameters for use with Connector for SCEP for Microsoft Intune. For more information about using Connector for SCEP for Microsoft Intune, see Using Connector for SCEP for Microsoft Intune.

Type: OpenIdConfiguration object

Required: No

Status

The connector's status.

Type: String

Valid Values: `CREATING | ACTIVE | DELETING | FAILED`

Required: No

StatusReason

Information about why connector creation failed, if status is `FAILED`.

Type: String

Valid Values: `INTERNAL_FAILURE | PRIVATECA_ACCESS_DENIED | PRIVATECA_INVALID_STATE | PRIVATECA_RESOURCE_NOT_FOUND`

Required: No

Type

The connector type.

Type: String

Valid Values: `GENERAL_PURPOSE | INTUNE`

Required: No

UpdatedAt

The date and time that the connector was updated.

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

ConnectorSummary

Lists the AWS Private CA SCEP connectors belonging to your AWS account.

Contents

Arn

The Amazon Resource Name (ARN) of the connector.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:pca-connector-scep:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CertificateAuthorityArn

The Amazon Resource Name (ARN) of the connector's associated certificate authority.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:aws(-[a-z]+)*:acm-pca:[a-z]+(-[a-z]+)+-[1-9]\d*:\d{12}:certificate-authority\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CreatedAt

The date and time that the challenge was created.

Type: Timestamp

Required: No

Endpoint

The connector's HTTPS public SCEP URL.

Type: String

Required: No

MobileDeviceManagement

Contains settings relevant to the mobile device management system that you chose for the connector. If you didn't configure `MobileDeviceManagement`, then the connector is for general-purpose use and this object is empty.

Type: MobileDeviceManagement object

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

Required: No

OpenIdConfiguration

Contains OpenID Connect (OIDC) parameters for use with Microsoft Intune.

Type: OpenIdConfiguration object

Required: No

Status

The connector's status. Status can be creating, active, deleting, or failed.

Type: String

Valid Values: `CREATING | ACTIVE | DELETING | FAILED`

Required: No

StatusReason

Information about why connector creation failed, if status is `FAILED`.

Type: String

Valid Values: `INTERNAL_FAILURE | PRIVATECA_ACCESS_DENIED | PRIVATECA_INVALID_STATE | PRIVATECA_RESOURCE_NOT_FOUND`

Required: No

Type

The connector type.

Type: String

Valid Values: `GENERAL_PURPOSE | INTUNE`

Required: No

UpdatedAt

The date and time that the challenge was updated.

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

IntuneConfiguration

Contains configuration details for use with Microsoft Intune. For information about using Connector for SCEP for Microsoft Intune, see Using Connector for SCEP for Microsoft Intune.

When you use Connector for SCEP for Microsoft Intune, certain functionalities are enabled by accessing Microsoft Intune through the Microsoft API. Your use of the Connector for SCEP and accompanying AWS services doesn't remove your need to have a valid license for your use of the Microsoft Intune service. You should also review the Microsoft Intune® App Protection Policies.

Contents

AzureApplicationId

The directory (tenant) ID from your Microsoft Entra ID app registration.

Type: String

Length Constraints: Minimum length of 15. Maximum length of 100.

Pattern: `[a-zA-Z0-9]{2,15}-[a-zA-Z0-9]{2,15}-[a-zA-Z0-9]{2,15}-[a-zA-Z0-9]{2,15}-[a-zA-Z0-9]{2,15}`

Required: Yes

Domain

The primary domain from your Microsoft Entra ID app registration.

Type: String

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

Pattern: `[a-zA-Z0-9._-]+`

Required: Yes

See Also

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

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

MobileDeviceManagement

If you don't supply a value, by default Connector for SCEP creates a connector for general-purpose use. A general-purpose connector is designed to work with clients or endpoints that support the SCEP protocol, except Connector for SCEP for Microsoft Intune. For information about considerations and limitations with using Connector for SCEP, see Considerations and Limitations.

If you provide an `IntuneConfiguration`, Connector for SCEP creates a connector for use with Microsoft Intune, and you manage the challenge passwords using Microsoft Intune. For more information, see Using Connector for SCEP for Microsoft Intune.

Contents

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

Intune

Configuration settings for use with Microsoft Intune. For information about using Connector for SCEP for Microsoft Intune, see Using Connector for SCEP for Microsoft Intune.

Type: IntuneConfiguration 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

OpenIdConfiguration

Contains OpenID Connect (OIDC) parameters for use with Microsoft Intune. For more information about using Connector for SCEP for Microsoft Intune, see Using Connector for SCEP for Microsoft Intune.

Contents

Audience

The audience value to copy into your Microsoft Entra app registration's OIDC.

Type: String

Required: No

Issuer

The issuer value to copy into your Microsoft Entra app registration's OIDC.

Type: String

Required: No

Subject

The subject value to copy into your Microsoft Entra app registration's OIDC.

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

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*.

Action

The action to be performed.

Type: string

Required: Yes

Version

The API version that the request is written for, expressed in the format YYYY-MM-DD.

Type: string

Required: Yes

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 Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ExpiredTokenException

The security token included in the request is expired

HTTP Status Code: 403

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 403

InternalFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

MalformedHttpRequestException

Problems with the request at the HTTP level, e.g. we can't decompress the body according to the decompression algorithm specified by the content-encoding.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 401

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestAbortedException

Convenient exception that can be used when a request is aborted before a reply is sent back (e.g. client closed connection).

HTTP Status Code: 400

RequestEntityTooLargeException

Problems with the request at the HTTP level. The request entity is too large.

HTTP Status Code: 413

RequestExpired

The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.

HTTP Status Code: 400

RequestTimeoutException

Problems with the request at the HTTP level. Reading the Request timed out.

HTTP Status Code: 408

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

UnrecognizedClientException

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

UnknownOperationException

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 404

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400