



API Reference

IAM Roles Anywhere



API Version 2018-05-10

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

IAM Roles Anywhere: API Reference

Copyright © 2025 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	2
CreateProfile	4
Request Syntax	4
URI Request Parameters	4
Request Body	4
Response Syntax	6
Response Elements	7
Errors	7
See Also	8
CreateTrustAnchor	9
Request Syntax	9
URI Request Parameters	9
Request Body	10
Response Syntax	11
Response Elements	11
Errors	12
See Also	12
DeleteAttributeMapping	13
Request Syntax	13
URI Request Parameters	13
Request Body	13
Response Syntax	13
Response Elements	14
Errors	15
See Also	15
DeleteCrl	16
Request Syntax	16
URI Request Parameters	16
Request Body	16
Response Syntax	16
Response Elements	17
Errors	17
See Also	17

DeleteProfile	19
Request Syntax	19
URI Request Parameters	19
Request Body	19
Response Syntax	19
Response Elements	20
Errors	20
See Also	21
DeleteTrustAnchor	22
Request Syntax	22
URI Request Parameters	22
Request Body	22
Response Syntax	22
Response Elements	23
Errors	23
See Also	24
DisableCrl	25
Request Syntax	25
URI Request Parameters	25
Request Body	25
Response Syntax	25
Response Elements	26
Errors	26
See Also	26
DisableProfile	28
Request Syntax	28
URI Request Parameters	28
Request Body	28
Response Syntax	28
Response Elements	29
Errors	29
See Also	30
DisableTrustAnchor	31
Request Syntax	31
URI Request Parameters	31
Request Body	31

Response Syntax	31
Response Elements	32
Errors	32
See Also	33
EnableCrl	34
Request Syntax	34
URI Request Parameters	34
Request Body	34
Response Syntax	34
Response Elements	35
Errors	35
See Also	35
EnableProfile	37
Request Syntax	37
URI Request Parameters	37
Request Body	37
Response Syntax	37
Response Elements	38
Errors	38
See Also	39
EnableTrustAnchor	40
Request Syntax	40
URI Request Parameters	40
Request Body	40
Response Syntax	40
Response Elements	41
Errors	41
See Also	42
GetCrl	43
Request Syntax	43
URI Request Parameters	43
Request Body	43
Response Syntax	43
Response Elements	44
Errors	44
See Also	44

GetProfile	46
Request Syntax	46
URI Request Parameters	46
Request Body	46
Response Syntax	46
Response Elements	47
Errors	47
See Also	48
GetSubject	49
Request Syntax	49
URI Request Parameters	49
Request Body	49
Response Syntax	49
Response Elements	50
Errors	50
See Also	51
GetTrustAnchor	52
Request Syntax	52
URI Request Parameters	52
Request Body	52
Response Syntax	52
Response Elements	53
Errors	53
See Also	54
ImportCrl	55
Request Syntax	55
URI Request Parameters	55
Request Body	55
Response Syntax	56
Response Elements	57
Errors	57
See Also	58
ListCrls	59
Request Syntax	59
URI Request Parameters	59
Request Body	59

Response Syntax	59
Response Elements	60
Errors	60
See Also	61
ListProfiles	62
Request Syntax	62
URI Request Parameters	62
Request Body	62
Response Syntax	62
Response Elements	63
Errors	64
See Also	64
ListSubjects	65
Request Syntax	65
URI Request Parameters	65
Request Body	65
Response Syntax	65
Response Elements	66
Errors	66
See Also	67
ListTagsForResource	68
Request Syntax	68
URI Request Parameters	68
Request Body	68
Response Syntax	68
Response Elements	69
Errors	69
See Also	69
ListTrustAnchors	71
Request Syntax	71
URI Request Parameters	71
Request Body	71
Response Syntax	71
Response Elements	72
Errors	72
See Also	73

PutAttributeMapping	74
Request Syntax	74
URI Request Parameters	74
Request Body	74
Response Syntax	75
Response Elements	76
Errors	76
See Also	76
PutNotificationSettings	78
Request Syntax	78
URI Request Parameters	78
Request Body	78
Response Syntax	79
Response Elements	80
Errors	80
See Also	80
ResetNotificationSettings	82
Request Syntax	82
URI Request Parameters	82
Request Body	82
Response Syntax	83
Response Elements	83
Errors	84
See Also	84
TagResource	86
Request Syntax	86
URI Request Parameters	86
Request Body	86
Response Syntax	87
Response Elements	87
Errors	87
See Also	88
UntagResource	89
Request Syntax	89
URI Request Parameters	89
Request Body	89

Response Syntax	90
Response Elements	90
Errors	90
See Also	90
UpdateCrl	92
Request Syntax	92
URI Request Parameters	92
Request Body	92
Response Syntax	93
Response Elements	93
Errors	94
See Also	94
UpdateProfile	96
Request Syntax	96
URI Request Parameters	96
Request Body	96
Response Syntax	98
Response Elements	99
Errors	99
See Also	100
UpdateTrustAnchor	101
Request Syntax	101
URI Request Parameters	101
Request Body	101
Response Syntax	102
Response Elements	103
Errors	103
See Also	103
Data Types	105
AttributeMapping	106
Contents	106
See Also	106
CredentialSummary	107
Contents	107
See Also	108
CrlDetail	109

Contents	109
See Also	110
InstanceProperty	111
Contents	111
See Also	111
MappingRule	113
Contents	113
See Also	113
NotificationSetting	114
Contents	114
See Also	115
NotificationSettingDetail	116
Contents	116
See Also	117
NotificationSettingKey	118
Contents	118
See Also	118
ProfileDetail	119
Contents	119
See Also	122
Source	123
Contents	123
See Also	123
SourceData	124
Contents	124
See Also	124
SubjectDetail	126
Contents	126
See Also	127
SubjectSummary	129
Contents	129
See Also	130
Tag	131
Contents	131
See Also	131
TrustAnchorDetail	132

Contents	132
See Also	133
Common Parameters	134
Common Errors	137

Welcome

AWS Identity and Access Management Roles Anywhere provides a secure way for your workloads such as servers, containers, and applications that run outside of AWS to obtain temporary AWS credentials. Your workloads can use the same IAM policies and roles you have for native AWS applications to access AWS resources. Using IAM Roles Anywhere eliminates the need to manage long-term credentials for workloads running outside of AWS.

To use IAM Roles Anywhere, your workloads must use X.509 certificates issued by their certificate authority (CA). You register the CA with IAM Roles Anywhere as a trust anchor to establish trust between your public key infrastructure (PKI) and IAM Roles Anywhere. If you don't manage your own PKI system, you can use AWS Private Certificate Authority to create a CA and then use that to establish trust with IAM Roles Anywhere.

This guide describes the IAM Roles Anywhere operations that you can call programmatically. For more information about IAM Roles Anywhere, see the [IAM Roles Anywhere User Guide](#).

This document was last published on July 22, 2025.

Actions

The following actions are supported:

- [CreateProfile](#)
- [CreateTrustAnchor](#)
- [DeleteAttributeMapping](#)
- [DeleteCrl](#)
- [DeleteProfile](#)
- [DeleteTrustAnchor](#)
- [DisableCrl](#)
- [DisableProfile](#)
- [DisableTrustAnchor](#)
- [EnableCrl](#)
- [EnableProfile](#)
- [EnableTrustAnchor](#)
- [GetCrl](#)
- [GetProfile](#)
- [GetSubject](#)
- [GetTrustAnchor](#)
- [ImportCrl](#)
- [ListCrls](#)
- [ListProfiles](#)
- [ListSubjects](#)
- [ListTagsForResource](#)
- [ListTrustAnchors](#)
- [PutAttributeMapping](#)
- [PutNotificationSettings](#)
- [ResetNotificationSettings](#)
- [TagResource](#)
- [UntagResource](#)

- [UpdateCrl](#)
- [UpdateProfile](#)
- [UpdateTrustAnchor](#)

CreateProfile

Creates a *profile*, a list of the roles that Roles Anywhere service is trusted to assume. You use profiles to intersect permissions with IAM managed policies.

Required permissions: rolesanywhere:CreateProfile.

Request Syntax

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

{
  "acceptRoleSessionName": boolean,
  "durationSeconds": number,
  "enabled": boolean,
  "managedPolicyArns": [ "string" ],
  "name": "string",
  "requireInstanceProperties": boolean,
  "roleArns": [ "string" ],
  "sessionPolicy": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

acceptRoleSessionName

Used to determine if a custom role session name will be accepted in a temporary credential request.

Type: Boolean

Required: No

durationSeconds

Used to determine how long sessions vended using this profile are valid for. See the Expiration section of the [CreateSession API documentation](#) page for more details. In requests, if this value is not provided, the default value will be 3600.

Type: Integer

Valid Range: Minimum value of 900. Maximum value of 43200.

Required: No

enabled

Specifies whether the profile is enabled.

Type: Boolean

Required: No

managedPolicyArns

A list of managed policy ARNs that apply to the vended session credentials.

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 200.

Required: No

name

The name of the profile.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: [a-zA-Z0-9-_*]*

Required: Yes

requireInstanceProperties

Unused, saved for future use. Will likely specify whether instance properties are required in temporary credential requests with this profile.

Type: Boolean

Required: No

roleArns

A list of IAM roles that this profile can assume in a temporary credential request.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 250 items.

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `arn:aws(-[^\:]+)?:iam(:.*){2}(:role.*)`

Required: Yes

sessionPolicy

A session policy that applies to the trust boundary of the vended session credentials.

Type: String

Required: No

tags

The tags to attach to the profile.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Syntax

```
HTTP/1.1 201
Content-type: application/json
```

```
{
  "profile": {
    "acceptRoleSessionName": boolean,
    "attributeMappings": [
      {
        "certificateField": "string",
        "mappingRules": [
          {
            "specifier": "string"
          }
        ]
      }
    ]
  },
  "createdAt": "string",
  "createdBy": "string",
  "durationSeconds": number,
  "enabled": boolean,
  "managedPolicyArns": [ "string" ],
  "name": "string",
  "profileArn": "string",
  "profileId": "string",
  "requireInstanceProperties": boolean,
  "roleArns": [ "string" ],
  "sessionPolicy": "string",
  "updatedAt": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

profile

The state of the profile after a read or write operation.

Type: [ProfileDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ValidationException

Validation exception error.

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](#)
- [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](#)

CreateTrustAnchor

Creates a trust anchor to establish trust between IAM Roles Anywhere and your certificate authority (CA). You can define a trust anchor as a reference to an AWS Private Certificate Authority (AWS Private CA) or by uploading a CA certificate. Your AWS workloads can authenticate with the trust anchor using certificates issued by the CA in exchange for temporary AWS credentials.

Required permissions: `rolesanywhere:CreateTrustAnchor`.

Request Syntax

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

```
{
  "enabled": boolean,
  "name": "string",
  "notificationSettings": [
    {
      "channel": "string",
      "enabled": boolean,
      "event": "string",
      "threshold": number
    }
  ],
  "source": {
    "sourceData": { ... },
    "sourceType": "string"
  },
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

enabled

Specifies whether the trust anchor is enabled.

Type: Boolean

Required: No

name

The name of the trust anchor.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: [a-zA-Z0-9-_*]*

Required: Yes

notificationSettings

A list of notification settings to be associated to the trust anchor.

Type: Array of [NotificationSetting](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: No

source

The trust anchor type and its related certificate data.

Type: [Source](#) object

Required: Yes

tags

The tags to attach to the trust anchor.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Syntax

```
HTTP/1.1 201
Content-type: application/json

{
  "trustAnchor": {
    "createdAt": "string",
    "enabled": boolean,
    "name": "string",
    "notificationSettings": [
      {
        "channel": "string",
        "configuredBy": "string",
        "enabled": boolean,
        "event": "string",
        "threshold": number
      }
    ],
    "source": {
      "sourceData": { ... },
      "sourceType": "string"
    },
    "trustAnchorArn": "string",
    "trustAnchorId": "string",
    "updatedAt": "string"
  }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

trustAnchor

The state of the trust anchor after a read or write operation.

Type: [TrustAnchorDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ValidationException

Validation exception error.

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](#)
- [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](#)

DeleteAttributeMapping

Delete an entry from the attribute mapping rules enforced by a given profile.

Request Syntax

```
DELETE /profiles/profileId/mappings?  
certificateField=certificateField&specifiers=specifiers HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

certificateField

Fields (x509Subject, x509Issuer and x509SAN) within X.509 certificates.

Valid Values: x509Subject | x509Issuer | x509SAN

Required: Yes

profileId

The unique identifier of the profile.

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

specifiers

A list of specifiers of a certificate field; for example, CN, OU, UID from a Subject.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```



```
Content-type: application/json

{
  "profile": {
    "acceptRoleSessionName": boolean,
    "attributeMappings": [
      {
        "certificateField": "string",
        "mappingRules": [
          {
            "specifier": "string"
          }
        ]
      }
    ],
    "createdAt": "string",
    "createdBy": "string",
    "durationSeconds": number,
    "enabled": boolean,
    "managedPolicyArns": [ "string" ],
    "name": "string",
    "profileArn": "string",
    "profileId": "string",
    "requireInstanceProperties": boolean,
    "roleArns": [ "string" ],
    "sessionPolicy": "string",
    "updatedAt": "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.

profile

The state of the profile after a read or write operation.

Type: [ProfileDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ValidationException

Validation exception error.

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](#)
- [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](#)

DeleteCrl

Deletes a certificate revocation list (CRL).

Required permissions: rolesanywhere:DeleteCrl.

Request Syntax

```
DELETE /crl/crlId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

crlId

The unique identifier of the certificate revocation list (CRL).

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
  "crl": {
    "createdAt": "string",
    "crlArn": "string",
    "crlData": blob,
    "crlId": "string",
    "enabled": boolean,
```

```
  "name": "string",  
  "trustAnchorArn": "string",  
  "updatedAt": "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.

crl

The state of the certificate revocation list (CRL) after a read or write operation.

Type: [CrlDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

See Also

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

- [AWS Command Line Interface](#)
- [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](#)

DeleteProfile

Deletes a profile.

Required permissions: rolesanywhere:DeleteProfile.

Request Syntax

```
DELETE /profile/profileId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

profileId

The unique identifier of the profile.

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
  "profile": {
    "acceptRoleSessionName": boolean,
    "attributeMappings": [
      {
        "certificateField": "string",
        "mappingRules": [
```

```
        {
          "specifier": "string"
        }
      ]
    }
  ],
  "createdAt": "string",
  "createdBy": "string",
  "durationSeconds": number,
  "enabled": boolean,
  "managedPolicyArns": [ "string" ],
  "name": "string",
  "profileArn": "string",
  "profileId": "string",
  "requireInstanceProperties": boolean,
  "roleArns": [ "string" ],
  "sessionPolicy": "string",
  "updatedAt": "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.

profile

The state of the profile after a read or write operation.

Type: [ProfileDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

See Also

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

- [AWS Command Line Interface](#)
- [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](#)

DeleteTrustAnchor

Deletes a trust anchor.

Required permissions: `rolesanywhere:DeleteTrustAnchor`.

Request Syntax

```
DELETE /trustanchor/trustAnchorId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

trustAnchorId

The unique identifier of the trust anchor.

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
  "trustAnchor": {
    "createdAt": "string",
    "enabled": boolean,
    "name": "string",
    "notificationSettings": [
      {
        "channel": "string",
```

```
    "configuredBy": "string",
    "enabled": boolean,
    "event": "string",
    "threshold": number
  }
],
"source": {
  "sourceData": { ... },
  "sourceType": "string"
},
"trustAnchorArn": "string",
"trustAnchorId": "string",
"updatedAt": "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.

trustAnchor

The state of the trust anchor after a read or write operation.

Type: [TrustAnchorDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

See Also

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

- [AWS Command Line Interface](#)
- [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](#)

DisableCrl

Disables a certificate revocation list (CRL).

Required permissions: rolesanywhere:DisableCrl.

Request Syntax

```
POST /crl/crlId/disable HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

crlId

The unique identifier of the certificate revocation list (CRL).

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
  "crl": {
    "createdAt": "string",
    "crlArn": "string",
    "crlData": blob,
    "crlId": "string",
    "enabled": boolean,
```

```
  "name": "string",  
  "trustAnchorArn": "string",  
  "updatedAt": "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.

crl

The state of the certificate revocation list (CRL) after a read or write operation.

Type: [CrlDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

See Also

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

- [AWS Command Line Interface](#)
- [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](#)

DisableProfile

Disables a profile. When disabled, temporary credential requests with this profile fail.

Required permissions: `rolesanywhere:DisableProfile`.

Request Syntax

```
POST /profile/profileId/disable HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

profileId

The unique identifier of the profile.

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
  "profile": {
    "acceptRoleSessionName": boolean,
    "attributeMappings": [
      {
        "certificateField": "string",
        "mappingRules": [
```

```
        {
          "specifier": "string"
        }
      ]
    }
  ],
  "createdAt": "string",
  "createdBy": "string",
  "durationSeconds": number,
  "enabled": boolean,
  "managedPolicyArns": [ "string" ],
  "name": "string",
  "profileArn": "string",
  "profileId": "string",
  "requireInstanceProperties": boolean,
  "roleArns": [ "string" ],
  "sessionPolicy": "string",
  "updatedAt": "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.

profile

The state of the profile after a read or write operation.

Type: [ProfileDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

See Also

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

- [AWS Command Line Interface](#)
- [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](#)

DisableTrustAnchor

Disables a trust anchor. When disabled, temporary credential requests specifying this trust anchor are unauthorized.

Required permissions: `rolesanywhere:DisableTrustAnchor`.

Request Syntax

```
POST /trustanchor/trustAnchorId/disable HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

trustAnchorId

The unique identifier of the trust anchor.

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
  "trustAnchor": {
    "createdAt": "string",
    "enabled": boolean,
    "name": "string",
    "notificationSettings": [
```

```
{
  "channel": "string",
  "configuredBy": "string",
  "enabled": boolean,
  "event": "string",
  "threshold": number
},
"source": {
  "sourceData": { ... },
  "sourceType": "string"
},
"trustAnchorArn": "string",
"trustAnchorId": "string",
"updatedAt": "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.

trustAnchor

The state of the trust anchor after a read or write operation.

Type: [TrustAnchorDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

See Also

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

- [AWS Command Line Interface](#)
- [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](#)

EnableCrl

Enables a certificate revocation list (CRL). When enabled, certificates stored in the CRL are unauthorized to receive session credentials.

Required permissions: `rolesanywhere:EnableCrl`.

Request Syntax

```
POST /crl/crlId/enable HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

crlId

The unique identifier of the certificate revocation list (CRL).

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

```
{
  "crl": {
    "createdAt": "string",
    "crlArn": "string",
    "crlData": blob,
    "crlId": "string",
```

```
"enabled": boolean,  
"name": "string",  
"trustAnchorArn": "string",  
"updatedAt": "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.

[crl](#)

The state of the certificate revocation list (CRL) after a read or write operation.

Type: [CrlDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

See Also

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

- [AWS Command Line Interface](#)

- [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](#)

EnableProfile

Enables temporary credential requests for a profile.

Required permissions: rolesanywhere:EnableProfile.

Request Syntax

```
POST /profile/profileId/enable HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

profileId

The unique identifier of the profile.

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
  "profile": {
    "acceptRoleSessionName": boolean,
    "attributeMappings": [
      {
        "certificateField": "string",
        "mappingRules": [
```



```
        {
          "specifier": "string"
        }
      ]
    }
  ],
  "createdAt": "string",
  "createdBy": "string",
  "durationSeconds": number,
  "enabled": boolean,
  "managedPolicyArns": [ "string" ],
  "name": "string",
  "profileArn": "string",
  "profileId": "string",
  "requireInstanceProperties": boolean,
  "roleArns": [ "string" ],
  "sessionPolicy": "string",
  "updatedAt": "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.

profile

The state of the profile after a read or write operation.

Type: [ProfileDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

See Also

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

- [AWS Command Line Interface](#)
- [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](#)

EnableTrustAnchor

Enables a trust anchor. When enabled, certificates in the trust anchor chain are authorized for trust validation.

Required permissions: `rolesanywhere:EnableTrustAnchor`.

Request Syntax

```
POST /trustanchor/trustAnchorId/enable HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

trustAnchorId

The unique identifier of the trust anchor.

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
  "trustAnchor": {
    "createdAt": "string",
    "enabled": boolean,
    "name": "string",
    "notificationSettings": [
```

```
{
  "channel": "string",
  "configuredBy": "string",
  "enabled": boolean,
  "event": "string",
  "threshold": number
},
{
  "source": {
    "sourceData": { ... },
    "sourceType": "string"
  },
  "trustAnchorArn": "string",
  "trustAnchorId": "string",
  "updatedAt": "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.

trustAnchor

The state of the trust anchor after a read or write operation.

Type: [TrustAnchorDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

See Also

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

- [AWS Command Line Interface](#)
- [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](#)

GetCrl

Gets a certificate revocation list (CRL).

Required permissions: rolesanywhere:GetCrl.

Request Syntax

```
GET /crl/crlId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

crlId

The unique identifier of the certificate revocation list (CRL).

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
  "crl": {
    "createdAt": "string",
    "crlArn": "string",
    "crlData": blob,
    "crlId": "string",
    "enabled": boolean,
```

```
    "name": "string",
    "trustAnchorArn": "string",
    "updatedAt": "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.

[crl](#)

The state of the certificate revocation list (CRL) after a read or write operation.

Type: [CrlDetail](#) object

Errors

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

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

See Also

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

- [AWS Command Line Interface](#)
- [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](#)

GetProfile

Gets a profile.

Required permissions: rolesanywhere:GetProfile.

Request Syntax

```
GET /profile/profileId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

profileId

The unique identifier of the profile.

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
  "profile": {
    "acceptRoleSessionName": boolean,
    "attributeMappings": [
      {
        "certificateField": "string",
        "mappingRules": [
```

```
        {
          "specifier": "string"
        }
      ]
    }
  ],
  "createdAt": "string",
  "createdBy": "string",
  "durationSeconds": number,
  "enabled": boolean,
  "managedPolicyArns": [ "string" ],
  "name": "string",
  "profileArn": "string",
  "profileId": "string",
  "requireInstanceProperties": boolean,
  "roleArns": [ "string" ],
  "sessionPolicy": "string",
  "updatedAt": "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.

profile

The state of the profile after a read or write operation.

Type: [ProfileDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

See Also

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

- [AWS Command Line Interface](#)
- [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](#)

GetSubject

Gets a *subject*, which associates a certificate identity with authentication attempts. The subject stores auditing information such as the status of the last authentication attempt, the certificate data used in the attempt, and the last time the associated identity attempted authentication.

Required permissions: `rolesanywhere:GetSubject`.

Request Syntax

```
GET /subject/subjectId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

subjectId

The unique identifier of the subject.

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
  "subject": {
    "createdAt": "string",
    "credentials": [
```

```
{
  {
    "enabled": boolean,
    "failed": boolean,
    "issuer": "string",
    "seenAt": "string",
    "serialNumber": "string",
    "x509CertificateData": "string"
  }
],
"enabled": boolean,
"instanceProperties": [
  {
    "failed": boolean,
    "properties": {
      "string" : "string"
    },
    "seenAt": "string"
  }
],
"lastSeenAt": "string",
"subjectArn": "string",
"subjectId": "string",
"updatedAt": "string",
"x509Subject": "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.

subject

The state of the subject after a read or write operation.

Type: [SubjectDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

See Also

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

- [AWS Command Line Interface](#)
- [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](#)

GetTrustAnchor

Gets a trust anchor.

Required permissions: `rolesanywhere:GetTrustAnchor`.

Request Syntax

```
GET /trustanchor/trustAnchorId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

trustAnchorId

The unique identifier of the trust anchor.

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
  "trustAnchor": {
    "createdAt": "string",
    "enabled": boolean,
    "name": "string",
    "notificationSettings": [
      {
        "channel": "string",
```

```
    "configuredBy": "string",
    "enabled": boolean,
    "event": "string",
    "threshold": number
  }
],
"source": {
  "sourceData": { ... },
  "sourceType": "string"
},
"trustAnchorArn": "string",
"trustAnchorId": "string",
"updatedAt": "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.

trustAnchor

The state of the trust anchor after a read or write operation.

Type: [TrustAnchorDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ValidationException

Validation exception error.

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](#)
- [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](#)

ImportCrl

Imports the certificate revocation list (CRL). A CRL is a list of certificates that have been revoked by the issuing certificate Authority (CA). In order to be properly imported, a CRL must be in PEM format. IAM Roles Anywhere validates against the CRL before issuing credentials.

Required permissions: `rolesanywhere:ImportCrl`.

Request Syntax

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

{
  "crlData": blob,
  "enabled": boolean,
  "name": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ],
  "trustAnchorArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

crlData

The x509 v3 specified certificate revocation list (CRL).

Type: Base64-encoded binary data object

Length Constraints: Minimum length of 1. Maximum length of 300000.

Required: Yes

enabled

Specifies whether the certificate revocation list (CRL) is enabled.

Type: Boolean

Required: No

name

The name of the certificate revocation list (CRL).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: [a-zA-Z0-9-_*]*

Required: Yes

tags

A list of tags to attach to the certificate revocation list (CRL).

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

trustAnchorArn

The ARN of the TrustAnchor the certificate revocation list (CRL) will provide revocation for.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: arn:aws(-[^\:]+)?:rolesanywhere(:.*){2}(:trust-anchor.*)

Required: Yes

Response Syntax

```
HTTP/1.1 201
```

```
Content-type: application/json

{
  "crl": {
    "createdAt": "string",
    "crlArn": "string",
    "crlData": blob,
    "crlId": "string",
    "enabled": boolean,
    "name": "string",
    "trustAnchorArn": "string",
    "updatedAt": "string"
  }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

crl

The state of the certificate revocation list (CRL) after a read or write operation.

Type: [CrlDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ValidationException

Validation exception error.

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](#)
- [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](#)

ListCrls

Lists all certificate revocation lists (CRL) in the authenticated account and AWS Region.

Required permissions: `rolesanywhere:ListCrls`.

Request Syntax

```
GET /crls?nextToken=nextToken&pageSize=pageSize HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

[nextToken](#)

A token that indicates where the output should continue from, if a previous request did not show all results. To get the next results, make the request again with this value.

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

[pageSize](#)

The number of resources in the paginated list.

Request Body

The request does not have a request body.

Response Syntax

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

{
  "crls": [
    {
      "createdAt": "string",
      "crlArn": "string",
      "crlData": blob,
      "crlId": "string",
```

```
    "enabled": boolean,
    "name": "string",
    "trustAnchorArn": "string",
    "updatedAt": "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.

crls

A list of certificate revocation lists (CRL).

Type: Array of [CrlDetail](#) objects

nextToken

A token that indicates where the output should continue from, if a previous request did not show all results. To get the next results, make the request again with this value.

Type: String

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ValidationException

Validation exception error.

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](#)
- [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](#)

ListProfiles

Lists all profiles in the authenticated account and AWS Region.

Required permissions: `rolesanywhere:ListProfiles`.

Request Syntax

```
GET /profiles?nextToken=nextToken&pageSize=pageSize HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

[nextToken](#)

A token that indicates where the output should continue from, if a previous request did not show all results. To get the next results, make the request again with this value.

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

[pageSize](#)

The number of resources in the paginated list.

Request Body

The request does not have a request body.

Response Syntax

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

{
  "nextToken": "string",
  "profiles": [
    {
      "acceptRoleSessionName": boolean,
      "attributeMappings": [
```

```
{
  {
    "certificateField": "string",
    "mappingRules": [
      {
        "specifier": "string"
      }
    ]
  }
],
"createdAt": "string",
"createdBy": "string",
"durationSeconds": number,
"enabled": boolean,
"managedPolicyArns": [ "string" ],
"name": "string",
"profileArn": "string",
"profileId": "string",
"requireInstanceProperties": boolean,
"roleArns": [ "string" ],
"sessionPolicy": "string",
"updatedAt": "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

A token that indicates where the output should continue from, if a previous request did not show all results. To get the next results, make the request again with this value.

Type: String

profiles

A list of profiles.

Type: Array of [ProfileDetail](#) objects

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ValidationException

Validation exception error.

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](#)
- [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](#)

ListSubjects

Lists the subjects in the authenticated account and AWS Region.

Required permissions: `rolesanywhere:ListSubjects`.

Request Syntax

```
GET /subjects?nextToken=nextToken&pageSize=pageSize HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

[nextToken](#)

A token that indicates where the output should continue from, if a previous request did not show all results. To get the next results, make the request again with this value.

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

[pageSize](#)

The number of resources in the paginated list.

Request Body

The request does not have a request body.

Response Syntax

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

{
  "nextToken": "string",
  "subjects": [
    {
      "createdAt": "string",
      "enabled": boolean,
```

```
    "lastSeenAt": "string",
    "subjectArn": "string",
    "subjectId": "string",
    "updatedAt": "string",
    "x509Subject": "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

A token that indicates where the output should continue from, if a previous request did not show all results. To get the next results, make the request again with this value.

Type: String

subjects

A list of subjects.

Type: Array of [SubjectSummary](#) objects

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ValidationException

Validation exception error.

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](#)
- [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

Lists the tags attached to the resource.

Required permissions: `rolesanywhere:ListTagsForResource`.

Request Syntax

```
GET /ListTagsForResource?resourceArn=resourceArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

resourceArn

The ARN of the resource.

Length Constraints: Minimum length of 1. Maximum length of 1011.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

```
{
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Response Elements

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

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

tags

A list of tags attached to the resource.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ValidationException

Validation exception error.

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](#)

- [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](#)

ListTrustAnchors

Lists the trust anchors in the authenticated account and AWS Region.

Required permissions: `rolesanywhere:ListTrustAnchors`.

Request Syntax

```
GET /trustanchors?nextToken=nextToken&pageSize=pageSize HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

[nextToken](#)

A token that indicates where the output should continue from, if a previous request did not show all results. To get the next results, make the request again with this value.

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

[pageSize](#)

The number of resources in the paginated list.

Request Body

The request does not have a request body.

Response Syntax

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

{
  "nextToken": "string",
  "trustAnchors": [
    {
      "createdAt": "string",
      "enabled": boolean,
```

```
"name": "string",
"notificationSettings": [
  {
    "channel": "string",
    "configuredBy": "string",
    "enabled": boolean,
    "event": "string",
    "threshold": number
  }
],
"source": {
  "sourceData": { ... },
  "sourceType": "string"
},
"trustAnchorArn": "string",
"trustAnchorId": "string",
"updatedAt": "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

A token that indicates where the output should continue from, if a previous request did not show all results. To get the next results, make the request again with this value.

Type: String

trustAnchors

A list of trust anchors.

Type: Array of [TrustAnchorDetail](#) objects

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ValidationException

Validation exception error.

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](#)
- [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](#)

PutAttributeMapping

Put an entry in the attribute mapping rules that will be enforced by a given profile. A mapping specifies a certificate field and one or more specifiers that have contextual meanings.

Request Syntax

```
PUT /profiles/profileId/mappings HTTP/1.1
Content-type: application/json

{
  "certificateField": "string",
  "mappingRules": [
    {
      "specifier": "string"
    }
  ]
}
```

URI Request Parameters

The request uses the following URI parameters.

profileId

The unique identifier of the profile.

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request accepts the following data in JSON format.

certificateField

Fields (x509Subject, x509Issuer and x509SAN) within X.509 certificates.

Type: String

Valid Values: x509Subject | x509Issuer | x509SAN

Required: Yes

mappingRules

A list of mapping entries for every supported specifier or sub-field.

Type: Array of [MappingRule](#) objects

Required: Yes

Response Syntax

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

{
  "profile": {
    "acceptRoleSessionName": boolean,
    "attributeMappings": [
      {
        "certificateField": "string",
        "mappingRules": [
          {
            "specifier": "string"
          }
        ]
      }
    ],
    "createdAt": "string",
    "createdBy": "string",
    "durationSeconds": number,
    "enabled": boolean,
    "managedPolicyArns": [ "string" ],
    "name": "string",
    "profileArn": "string",
    "profileId": "string",
    "requireInstanceProperties": boolean,
    "roleArns": [ "string" ],
    "sessionPolicy": "string",
```

```
    "updatedAt": "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.

profile

The state of the profile after a read or write operation.

Type: [ProfileDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ValidationException

Validation exception error.

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](#)
- [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](#)

PutNotificationSettings

Attaches a list of *notification settings* to a trust anchor.

A notification setting includes information such as event name, threshold, status of the notification setting, and the channel to notify.

Required permissions: rolesanywhere:PutNotificationSettings.

Request Syntax

```
PATCH /put-notifications-settings HTTP/1.1
Content-type: application/json
```

```
{
  "notificationSettings": [
    {
      "channel": "string",
      "enabled": boolean,
      "event": "string",
      "threshold": number
    }
  ],
  "trustAnchorId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

notificationSettings

A list of notification settings to be associated to the trust anchor.

Type: Array of [NotificationSetting](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: Yes

trustAnchorId

The unique identifier of the trust anchor.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Response Syntax

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

{
  "trustAnchor": {
    "createdAt": "string",
    "enabled": boolean,
    "name": "string",
    "notificationSettings": [
      {
        "channel": "string",
        "configuredBy": "string",
        "enabled": boolean,
        "event": "string",
        "threshold": number
      }
    ],
    "source": {
      "sourceData": { ... },
      "sourceType": "string"
    },
    "trustAnchorArn": "string",
    "trustAnchorId": "string",
    "updatedAt": "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.

[trustAnchor](#)

The state of the trust anchor after a read or write operation.

Type: [TrustAnchorDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ValidationException

Validation exception error.

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](#)
- [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](#)

ResetNotificationSettings

Resets the *custom notification setting* to IAM Roles Anywhere default setting.

Required permissions: rolesanywhere:ResetNotificationSettings.

Request Syntax

```
PATCH /reset-notifications-settings HTTP/1.1
Content-type: application/json

{
  "notificationSettingKeys": [
    {
      "channel": "string",
      "event": "string"
    }
  ],
  "trustAnchorId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

notificationSettingKeys

A list of notification setting keys to reset. A notification setting key includes the event and the channel.

Type: Array of [NotificationSettingKey](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: Yes

trustAnchorId

The unique identifier of the trust anchor.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Response Syntax

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

{
  "trustAnchor": {
    "createdAt": "string",
    "enabled": boolean,
    "name": "string",
    "notificationSettings": [
      {
        "channel": "string",
        "configuredBy": "string",
        "enabled": boolean,
        "event": "string",
        "threshold": number
      }
    ],
    "source": {
      "sourceData": { ... },
      "sourceType": "string"
    },
    "trustAnchorArn": "string",
    "trustAnchorId": "string",
    "updatedAt": "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.

[trustAnchor](#)

The state of the trust anchor after a read or write operation.

Type: [TrustAnchorDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ValidationException

Validation exception error.

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](#)
- [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

Attaches tags to a resource.

Required permissions: rolesanywhere:TagResource.

Request Syntax

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

```
{
  "resourceArn": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

resourceArn

The ARN of the resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Required: Yes

tags

The tags to attach to the resource.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: Yes

Response Syntax

```
HTTP/1.1 201
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response with an empty HTTP body.

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

TooManyTagsException

Too many tags.

HTTP Status Code: 400

ValidationException

Validation exception error.

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](#)
- [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 tags from the resource.

Required permissions: rolesanywhere:UntagResource.

Request Syntax

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

```
{
  "resourceArn": "string",
  "tagKeys": [ "string" ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

resourceArn

The ARN of the resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Required: Yes

tagKeys

A list of keys. Tag keys are the unique identifiers of tags.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 200 items.

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

Pattern: [a-zA-Z0-9_ . : / = + @ -]*

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

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 Errors](#).

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ValidationException

Validation exception error.

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](#)
- [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](#)

UpdateCrl

Updates the certificate revocation list (CRL). A CRL is a list of certificates that have been revoked by the issuing certificate authority (CA). IAM Roles Anywhere validates against the CRL before issuing credentials.

Required permissions: `rolesanywhere:UpdateCrl`.

Request Syntax

```
PATCH /crl/crlId HTTP/1.1
Content-type: application/json

{
  "crlData": blob,
  "name": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

crlId

The unique identifier of the certificate revocation list (CRL).

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request accepts the following data in JSON format.

crlData

The x509 v3 specified certificate revocation list (CRL).

Type: Base64-encoded binary data object

Length Constraints: Minimum length of 1. Maximum length of 300000.

Required: No

name

The name of the Crl.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: [a-zA-Z0-9-_*]*

Required: No

Response Syntax

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

{
  "crl": {
    "createdAt": "string",
    "crlArn": "string",
    "crlData": blob,
    "crlId": "string",
    "enabled": boolean,
    "name": "string",
    "trustAnchorArn": "string",
    "updatedAt": "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.

crl

The state of the certificate revocation list (CRL) after a read or write operation.

Type: [CrlDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ValidationException

Validation exception error.

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](#)
- [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](#)

UpdateProfile

Updates a *profile*, a list of the roles that IAM Roles Anywhere service is trusted to assume. You use profiles to intersect permissions with IAM managed policies.

Required permissions: rolesanywhere:UpdateProfile.

Request Syntax

```
PATCH /profile/profileId HTTP/1.1
Content-type: application/json

{
  "acceptRoleSessionName": boolean,
  "durationSeconds": number,
  "managedPolicyArns": [ "string" ],
  "name": "string",
  "roleArns": [ "string" ],
  "sessionPolicy": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

profileId

The unique identifier of the profile.

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request accepts the following data in JSON format.

acceptRoleSessionName

Used to determine if a custom role session name will be accepted in a temporary credential request.

Type: Boolean

Required: No

durationSeconds

Used to determine how long sessions vended using this profile are valid for. See the Expiration section of the [CreateSession API documentation](#) page for more details. In requests, if this value is not provided, the default value will be 3600.

Type: Integer

Valid Range: Minimum value of 900. Maximum value of 43200.

Required: No

managedPolicyArns

A list of managed policy ARNs that apply to the vended session credentials.

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 200.

Required: No

name

The name of the profile.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: [a-zA-Z0-9-_*]*

Required: No

roleArns

A list of IAM roles that this profile can assume in a temporary credential request.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 250 items.

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `arn:aws(-[^\:]+)?:iam(:.*){2}(:role.*)`

Required: No

sessionPolicy

A session policy that applies to the trust boundary of the vended session credentials.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100000.

Required: No

Response Syntax

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

{
  "profile": {
    "acceptRoleSessionName": boolean,
    "attributeMappings": [
      {
        "certificateField": "string",
        "mappingRules": [
          {
            "specifier": "string"
          }
        ]
      }
    ]
  },
  "createdAt": "string",
  "createdBy": "string",
```

```
"durationSeconds": number,
"enabled": boolean,
"managedPolicyArns": [ "string" ],
"name": "string",
"profileArn": "string",
"profileId": "string",
"requireInstanceProperties": boolean,
"roleArns": [ "string" ],
"sessionPolicy": "string",
"updatedAt": "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.

profile

The state of the profile after a read or write operation.

Type: [ProfileDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ValidationException

Validation exception error.

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](#)
- [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](#)

UpdateTrustAnchor

Updates a trust anchor. You establish trust between IAM Roles Anywhere and your certificate authority (CA) by configuring a trust anchor. You can define a trust anchor as a reference to an AWS Private Certificate Authority (AWS Private CA) or by uploading a CA certificate. Your AWS workloads can authenticate with the trust anchor using certificates issued by the CA in exchange for temporary AWS credentials.

Required permissions: `rolesanywhere:UpdateTrustAnchor`.

Request Syntax

```
PATCH /trustanchor/trustAnchorId HTTP/1.1  
Content-type: application/json
```

```
{  
  "name": "string",  
  "source": {  
    "sourceData": { ... },  
    "sourceType": "string"  
  }  
}
```

URI Request Parameters

The request uses the following URI parameters.

trustAnchorId

The unique identifier of the trust anchor.

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: Yes

Request Body

The request accepts the following data in JSON format.

name

The name of the trust anchor.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: [a-zA-Z0-9-_*]*

Required: No

source

The trust anchor type and its related certificate data.

Type: [Source](#) object

Required: No

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json
```

```
{
  "trustAnchor": {
    "createdAt": "string",
    "enabled": boolean,
    "name": "string",
    "notificationSettings": [
      {
        "channel": "string",
        "configuredBy": "string",
        "enabled": boolean,
        "event": "string",
        "threshold": number
      }
    ],
    "source": {
      "sourceData": { ... },
      "sourceType": "string"
    },
    "trustAnchorArn": "string",
```

```
    "trustAnchorId": "string",
    "updatedAt": "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.

trustAnchor

The state of the trust anchor after a read or write operation.

Type: [TrustAnchorDetail](#) object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ValidationException

Validation exception error.

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](#)
- [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 IAM Roles Anywhere 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:

- [AttributeMapping](#)
- [CredentialSummary](#)
- [CrlDetail](#)
- [InstanceProperty](#)
- [MappingRule](#)
- [NotificationSetting](#)
- [NotificationSettingDetail](#)
- [NotificationSettingKey](#)
- [ProfileDetail](#)
- [Source](#)
- [SourceData](#)
- [SubjectDetail](#)
- [SubjectSummary](#)
- [Tag](#)
- [TrustAnchorDetail](#)

AttributeMapping

A mapping applied to the authenticating end-entity certificate.

Contents

`certificateField`

Fields (x509Subject, x509Issuer and x509SAN) within X.509 certificates.

Type: String

Valid Values: x509Subject | x509Issuer | x509SAN

Required: No

`mappingRules`

A list of mapping entries for every supported specifier or sub-field.

Type: Array of [MappingRule](#) objects

Required: No

See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CredentialSummary

A record of a presented X509 credential from a temporary credential request.

Contents

enabled

Indicates whether the credential is enabled.

Type: Boolean

Required: No

failed

Indicates whether the temporary credential request was successful.

Type: Boolean

Required: No

issuer

The fully qualified domain name of the issuing certificate for the presented end-entity certificate.

Type: String

Required: No

seenAt

The ISO-8601 time stamp of when the certificate was last used in a temporary credential request.

Type: Timestamp

Required: No

serialNumber

The serial number of the certificate.

Type: String

Required: No

x509CertificateData

The PEM-encoded data of the certificate.

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](#)

CrlDetail

The state of the certificate revocation list (CRL) after a read or write operation.

Contents

createdAt

The ISO-8601 timestamp when the certificate revocation list (CRL) was created.

Type: Timestamp

Required: No

crlArn

The ARN of the certificate revocation list (CRL).

Type: String

Required: No

crlData

The state of the certificate revocation list (CRL) after a read or write operation.

Type: Base64-encoded binary data object

Required: No

crlId

The unique identifier of the certificate revocation list (CRL).

Type: String

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: No

enabled

Indicates whether the certificate revocation list (CRL) is enabled.

Type: Boolean

Required: No

name

The name of the certificate revocation list (CRL).

Type: String

Required: No

trustAnchorArn

The ARN of the TrustAnchor the certificate revocation list (CRL) will provide revocation for.

Type: String

Required: No

updatedAt

The ISO-8601 timestamp when the certificate revocation list (CRL) was last 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](#)

InstanceProperty

A key-value pair you set that identifies a property of the authenticating instance.

Contents

failed

Indicates whether the temporary credential request was successful.

Type: Boolean

Required: No

properties

A list of instanceProperty objects.

Type: String to string map

Map Entries: Minimum number of 0 items. Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 200.

Value Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

seenAt

The ISO-8601 time stamp of when the certificate was last used in a temporary credential request.

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](#)

MappingRule

A single mapping entry for each supported specifier or sub-field.

Contents

specifier

Specifier within a certificate field, such as CN, OU, or UID from the Subject field.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 60.

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](#)

NotificationSetting

Customizable notification settings that will be applied to notification events. IAM Roles Anywhere consumes these settings while notifying across multiple channels - CloudWatch metrics, EventBridge, and AWS Health Dashboard.

Contents

enabled

Indicates whether the notification setting is enabled.

Type: Boolean

Required: Yes

event

The event to which this notification setting is applied.

Type: String

Valid Values: CA_CERTIFICATE_EXPIRY | END_ENTITY_CERTIFICATE_EXPIRY

Required: Yes

channel

The specified channel of notification. IAM Roles Anywhere uses CloudWatch metrics, EventBridge, and AWS Health Dashboard to notify for an event.

Note

In the absence of a specific channel, IAM Roles Anywhere applies this setting to 'ALL' channels.

Type: String

Valid Values: ALL

Required: No

threshold

The number of days before a notification event. This value is required for a notification setting that is enabled.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 360.

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](#)

NotificationSettingDetail

The state of a notification setting.

A notification setting includes information such as event name, threshold, status of the notification setting, and the channel to notify.

Contents

enabled

Indicates whether the notification setting is enabled.

Type: Boolean

Required: Yes

event

The event to which this notification setting is applied.

Type: String

Valid Values: CA_CERTIFICATE_EXPIRY | END_ENTITY_CERTIFICATE_EXPIRY

Required: Yes

channel

The specified channel of notification. IAM Roles Anywhere uses CloudWatch metrics, EventBridge, and AWS Health Dashboard to notify for an event.

Note

In the absence of a specific channel, IAM Roles Anywhere applies this setting to 'ALL' channels.

Type: String

Valid Values: ALL

Required: No

configuredBy

The principal that configured the notification setting. For default settings configured by IAM Roles Anywhere, the value is `rolesanywhere.amazonaws.com`, and for customized notifications settings, it is the respective account ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

threshold

The number of days before a notification event.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 360.

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](#)

NotificationSettingKey

A notification setting key to reset. A notification setting key includes the event and the channel.

Contents

event

The notification setting event to reset.

Type: String

Valid Values: CA_CERTIFICATE_EXPIRY | END_ENTITY_CERTIFICATE_EXPIRY

Required: Yes

channel

The specified channel of notification.

Type: String

Valid Values: ALL

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](#)

ProfileDetail

The state of the profile after a read or write operation.

Contents

acceptRoleSessionName

Used to determine if a custom role session name will be accepted in a temporary credential request.

Type: Boolean

Required: No

attributeMappings

A mapping applied to the authenticating end-entity certificate.

Type: Array of [AttributeMapping](#) objects

Required: No

createdAt

The ISO-8601 timestamp when the profile was created.

Type: Timestamp

Required: No

createdBy

The AWS account that created the profile.

Type: String

Required: No

durationSeconds

Used to determine how long sessions vended using this profile are valid for. See the [Expiration](#) section of the [CreateSession API documentation](#) page for more details. In requests, if this value is not provided, the default value will be 3600.

Type: Integer

Required: No

enabled

Indicates whether the profile is enabled.

Type: Boolean

Required: No

managedPolicyArns

A list of managed policy ARNs that apply to the vended session credentials.

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 200.

Required: No

name

The name of the profile.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: [a-zA-Z0-9-_*]*

Required: No

profileArn

The ARN of the profile.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: arn:aws(-[^:]+)?:rolesanywhere(:.*)_2(:profile.*)

Required: No

profileId

The unique identifier of the profile.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: No

requireInstanceProperties

Unused, saved for future use. Will likely specify whether instance properties are required in temporary credential requests with this profile.

Type: Boolean

Required: No

roleArns

A list of IAM roles that this profile can assume in a temporary credential request.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 250 items.

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `arn:aws(-[^\:]+)?:iam(:.*)" {2}(:role.*)`

Required: No

sessionPolicy

A session policy that applies to the trust boundary of the vended session credentials.

Type: String

Required: No

updatedAt

The ISO-8601 timestamp when the profile was last 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](#)

Source

The trust anchor type and its related certificate data.

Contents

sourceData

The data field of the trust anchor depending on its type.

Type: [SourceData](#) object

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

Required: No

sourceType

The type of the trust anchor.

Type: String

Valid Values: AWS_ACM_PCA | CERTIFICATE_BUNDLE | SELF_SIGNED_REPOSITORY

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](#)

SourceData

The data field of the trust anchor depending on its type.

Contents

Important

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

acmPcaArn

The root certificate of the AWS Private Certificate Authority specified by this ARN is used in trust validation for temporary credential requests. Included for trust anchors of type `AWS_ACM_PCA`.

Type: String

Required: No

x509CertificateData

The PEM-encoded data for the certificate anchor. Included for trust anchors of type `CERTIFICATE_BUNDLE`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 8000.

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](#)

SubjectDetail

The state of the subject after a read or write operation.

Contents

createdAt

The ISO-8601 timestamp when the subject was created.

Type: Timestamp

Required: No

credentials

The temporary session credentials vended at the last authenticating call with this subject.

Type: Array of [CredentialSummary](#) objects

Required: No

enabled

The enabled status of the subject.

Type: Boolean

Required: No

instanceProperties

The specified instance properties associated with the request.

Type: Array of [InstanceProperty](#) objects

Required: No

lastSeenAt

The ISO-8601 timestamp of the last time this subject requested temporary session credentials.

Type: Timestamp

Required: No

subjectArn

The ARN of the resource.

Type: String

Required: No

subjectId

The id of the resource

Type: String

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: No

updatedAt

The ISO-8601 timestamp when the subject was last updated.

Type: Timestamp

Required: No

x509Subject

The x509 principal identifier of the authenticating certificate.

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](#)

SubjectSummary

A summary representation of subjects.

Contents

createdAt

The ISO-8601 time stamp of when the certificate was first used in a temporary credential request.

Type: Timestamp

Required: No

enabled

The enabled status of the subject.

Type: Boolean

Required: No

lastSeenAt

The ISO-8601 time stamp of when the certificate was last used in a temporary credential request.

Type: Timestamp

Required: No

subjectArn

The ARN of the resource.

Type: String

Required: No

subjectId

The id of the resource.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: No

updatedAt

The ISO-8601 timestamp when the subject was last updated.

Type: Timestamp

Required: No

x509Subject

The x509 principal identifier of the authenticating certificate.

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](#)

Tag

A label that consists of a key and value you define.

Contents

key

The tag key.

Type: String

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

Pattern: [a-zA-Z0-9_./=+@-]*

Required: Yes

value

The tag value.

Type: String

Length Constraints: Minimum length of 0. 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](#)

TrustAnchorDetail

The state of the trust anchor after a read or write operation.

Contents

createdAt

The ISO-8601 timestamp when the trust anchor was created.

Type: Timestamp

Required: No

enabled

Indicates whether the trust anchor is enabled.

Type: Boolean

Required: No

name

The name of the trust anchor.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: [a-zA-Z0-9-_*]*

Required: No

notificationSettings

A list of notification settings to be associated to the trust anchor.

Type: Array of [NotificationSettingDetail](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: No

source

The trust anchor type and its related certificate data.

Type: [Source](#) object

Required: No

trustAnchorArn

The ARN of the trust anchor.

Type: String

Required: No

trustAnchorId

The unique identifier of the trust anchor.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `.*[a-f0-9]{8}-([a-z0-9]{4}-){3}[a-z0-9]{12}.*`

Required: No

updatedAt

The ISO-8601 timestamp when the trust anchor was last 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](#)

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