Welcome

# AWS Sign-In

# AWS Sign-In: Welcome

# Table of Contents

# Welcome

## AWS Sign-In Control Plane

With AWS Sign-In, you can access AWS resources using an AWS Builder ID, or as a root user, IAM user, user in IAM Identity Center, or federated user. For more information about how to sign in to AWS depending on your user type, see What is AWS Sign-In?.

This guide provides information about API actions for identity-aware sessions. For more information, see Enabling identity-aware console sessions.

> **Note**
>
> AWS Sign-In uses the `signin` namespace.

## AWS Sign-In Data Plane

The AWS Sign-In Data Plane implements OAuth 2.0 flows for AWS CLI authentication, providing secure token exchange and refresh capabilities.

> **Note**
>
> AWS Sign-In Data Plane uses the `signin` namespace.

# Actions

The following actions are supported by AWS Sign-In Control Plane:

- CreateTrustedIdentityPropagationApplicationForConsole
- DeleteConsoleAuthorizationConfiguration
- DeleteResourcePermissionStatement
- GetConsoleAuthorizationConfiguration
- GetResourcePolicy
- ListResourcePermissionStatements
- ListTrustedIdentityPropagationApplicationsForConsole
- PutConsoleAuthorizationConfiguration
- PutResourcePermissionStatement

The following actions are supported by AWS Sign-In Data Plane:

- AuthorizeOAuth2Access
- CreateOAuth2PublicClient
- CreateOAuth2Token
- CreateOAuth2TokenWithIAM
- IntrospectOAuth2TokenWithIAM
- RevokeOAuth2TokenWithIAM

# AWS Sign-In Control Plane

The following actions are supported by AWS Sign-In Control Plane:

- CreateTrustedIdentityPropagationApplicationForConsole
- DeleteConsoleAuthorizationConfiguration
- DeleteResourcePermissionStatement
- GetConsoleAuthorizationConfiguration
- GetResourcePolicy

- ListResourcePermissionStatements
- ListTrustedIdentityPropagationApplicationsForConsole
- PutConsoleAuthorizationConfiguration
- PutResourcePermissionStatement

# CreateTrustedIdentityPropagationApplicationForConsole

Service: AWS Sign-In Control Plane

Creates an IAM Identity Center application that represents the AWS Management Console on an IAM Identity Center organization instance. This application supports identity-aware sessions in IAM Identity Center, which enables additional user context to be included in the user's AWS Management Console session.

## Request Syntax

```
{
   "identityCenterInstanceArn": "string"
}
```

## Request Parameters

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

The request accepts the following data in JSON format.

### identityCenterInstanceArn

The ARN of the instance of IAM Identity Center under which the operation will run. For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 10. Maximum length of 1224.

Pattern: `arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):sso:::instance/(sso)?ins-[a-zA-Z0-9-.]{16}`

Required: Yes

## Response Syntax

```
{
   "applicationArn": "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.

**applicationArn**

Specifies the ARN of the newly created application.

Type: String

Length Constraints: Minimum length of 10. Maximum length of 1224.

Pattern: `arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):sso::[0-9]{12}:application/(sso)?ins-[a-zA-Z0-9-.]{16}/apl-[a-zA-Z0-9]{16}`

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**SetupFailedException**

The request to set up an IAM Identity Center application that represents the AWS Management Console has failed due to one of the following:

- `LIMIT_EXCEEDED` - Indicates that the principal has crossed the permitted number of resources that can be created.
- `RESOURCE_NOT_FOUND` - Indicates that the ARN of an instance of IAM Identity Center is not found.

- `APPLICATION_ALREADY_EXISTS` - Indicates that an IAM Identity Center application that represents the AWS Management Console already exists.

HTTP Status Code: 400

**ThrottlingException**

Indicates that the principal has crossed the throttling limits of the API operations.

HTTP Status Code: 400

**ValidationException**

The request failed because it contains a syntax 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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

# DeleteConsoleAuthorizationConfiguration

Service: AWS Sign-In Control Plane

Disables AWS Management Console authorization configuration for an AWS account or organization. The operation automatically detects whether the `targetId` is an account ID or an organization ID.

## Request Syntax

```
{
   "targetId": "string"
}
```

## Request Parameters

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

The request accepts the following data in JSON format.

### targetId

The target identifier whose AWS Management Console authorization configuration should be disabled. Accepts a 12-digit account ID, an organization ID (`o-xxxxxxxxxx`), or null/empty to use the caller's account ID.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 32.

Pattern: `(\d{12}|o-[a-z0-9]{10}|r-[0-9a-z]{4,32})`

Required: No

## Response Syntax

```
{
   "consoleAuthorizationEnabled": boolean,
   "scope": "string",
   "targetId": "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.

**consoleAuthorizationEnabled**

Indicates whether AWS Management Console authorization is enabled for the target. After a successful delete, this is `false`.

Type: Boolean

**scope**

The scope of the configuration that was deleted. Indicates whether the operation was applied at the account or organization level.

Type: String

**targetId**

The target identifier the configuration applied to.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 32.

Pattern: `(\d{12}|o-[a-z0-9]{10}|r-[0-9a-z]{4,32})`

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**ResourceNotFoundException**

The request was denied because the specified resource was not found.

HTTP Status Code: 400

**TooManyRequestsError**

The request was denied due to rate limiting.

HTTP Status Code: 400

**ValidationException**

The request failed because it contains a syntax 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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

# DeleteResourcePermissionStatement

Service: AWS Sign-In Control Plane

Removes a permission statement from the account's AWS Sign-In resource-based policy.

## Request Syntax

```
{
   "clientToken": "string",
   "statementId": "string"
}
```

## Request Parameters

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

The request accepts the following data in JSON format.

**clientToken**

A unique, case-sensitive identifier that you provide to ensure the idempotency of the request. If not provided, the AWS SDK will automatically generate one for you.

Type: String

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

Pattern: `[!-~]+`

Required: No

**statementId**

The unique identifier of the permission statement to delete.

Type: String

Pattern: `[A-Za-z0-9+/]{64}=?`

Required: Yes

## Response Elements

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

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**ResourceNotFoundException**

The request was denied because the specified resource was not found.

HTTP Status Code: 400

**TooManyRequestsError**

The request was denied due to rate limiting.

HTTP Status Code: 400

**ValidationException**

The request failed because it contains a syntax 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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2

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

# GetConsoleAuthorizationConfiguration

Service: AWS Sign-In Control Plane

Retrieves AWS Management Console authorization configuration for an AWS account or organization. The operation automatically detects whether the `targetId` is an account ID or an organization ID.

## Request Syntax

```
{
   "targetId": "string"
}
```

## Request Parameters

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

The request accepts the following data in JSON format.

**targetId**

The target identifier to retrieve the configuration for. Accepts a 12-digit account ID, an organization ID (`o-xxxxxxxxxx`), or null/empty to use the caller's account ID.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 32.

Pattern: `(\d{12}|o-[a-z0-9]{10}|r-[0-9a-z]{4,32})`

Required: No

## Response Syntax

```
{
   "consoleAuthorizationEnabled": boolean,
   "scope": "string",
   "targetId": "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.

**consoleAuthorizationEnabled**

Indicates whether AWS Management Console authorization is enabled for the target.

Type: Boolean

**scope**

The scope of the configuration. Indicates whether the configuration applies at the account or organization level.

Type: String

**targetId**

The target identifier the configuration applies to.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 32.

Pattern: `(\d{12}|o-[a-z0-9]{10}|r-[0-9a-z]{4,32})`

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**ResourceNotFoundException**

The request was denied because the specified resource was not found.

HTTP Status Code: 400

**TooManyRequestsError**

The request was denied due to rate limiting.

HTTP Status Code: 400

**ValidationException**

The request failed because it contains a syntax 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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

# GetResourcePolicy

Service: AWS Sign-In Control Plane

Retrieves the account's consolidated AWS Sign-In resource-based policy. Returns the complete policy document that aggregates all permission statements into a single policy.

## Response Syntax

```
{
   "signinResourceBasedPolicy": {
      "statement": [
         {
            "action": [ "string" ],
            "condition": {
               "string" : {
                  "string" : [ "string" ]
               }
            },
            "effect": "string",
            "principal": {
               "string" : "string"
            },
            "resource": "string"
         }
      ],
      "version": "string"
   }
}
```

## Response Elements

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

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

**signinResourceBasedPolicy**

The consolidated AWS Sign-In resource-based policy for the account.

Type: SigninResourceBasedPolicy object

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**ResourceNotFoundException**

The request was denied because the specified resource was not found.

HTTP Status Code: 400

**TooManyRequestsError**

The request was denied due to rate limiting.

HTTP Status Code: 400

## See Also

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

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

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

# ListResourcePermissionStatements

Service: AWS Sign-In Control Plane

Retrieves all permission statements in the account's AWS Sign-In resource-based policy.

## Request Syntax

```
{
   "maxResults": number,
   "nextToken": "string"
}
```

## Request Parameters

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

The request accepts the following data in JSON format.

**maxResults**

The maximum number of permission statements to return in a single response. Valid range is 1 to 100.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

**nextToken**

A pagination token that you can use in a subsequent call to retrieve the next set of results. Initially the value is null. Set this parameter to the value provided by the previous call's response to request the next page of results.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

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

Required: No

## Response Syntax

```
{
   "nextToken": "string",
   "permissionStatements": [
      {
         "condition": {
            "string" : {
               "string" : [ "string" ]
            }
         },
         "sid": "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**

If present, this value indicates that more output is available than is included in the current response. Use this value in the `nextToken` request parameter in a subsequent call to retrieve the next page of results.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

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

**permissionStatements**

A list of summaries of the permission statements in the AWS Sign-In resource-based policy.

Type: Array of PermissionStatementSummary objects

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**ResourceNotFoundException**

The request was denied because the specified resource was not found.

HTTP Status Code: 400

**TooManyRequestsError**

The request was denied due to rate limiting.

HTTP Status Code: 400

**ValidationException**

The request failed because it contains a syntax 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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

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

# ListTrustedIdentityPropagationApplicationsForConsole

Service: AWS Sign-In Control Plane

Lists an IAM Identity Center application that represents the AWS Management Console.

## Request Syntax

```
{
   "identityCenterInstanceArn": "string",
   "maxResults": number,
   "nextToken": "string"
}
```

## Request Parameters

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

The request accepts the following data in JSON format.

**identityCenterInstanceArn**

The ARN of the instance of IAM Identity Center under which the operation will run. For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 10. Maximum length of 1224.

Pattern: `arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):sso:::instance/(sso)?ins-[a-zA-Z0-9-.]{16}`

Required: Yes

**maxResults**

The maximum number of results to display for the instance.

Type: Integer

Valid Range: Fixed value of 1.

Required: No

**nextToken**

Specifies that you want to receive the next page of results. Initially the value is null. Valid only if you received a `NextToken` response in the previous request. If you did, it indicates that more output is available. Set this parameter to the value provided by the previous call's `NextToken` response to request the next page of results.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

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

Required: No

## Response Syntax

```
{
   "applicationArns": [ "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.

**applicationArns**

Specifies the ARNs for all of your IAM Identity Center applications that represent the AWS Management Console.

Type: Array of strings

Length Constraints: Minimum length of 10. Maximum length of 1224.

Pattern: `arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):sso::[0-9]{12}:application/(sso)?ins-[a-zA-Z0-9-.]{16}/apl-[a-zA-Z0-9]{16}`

**nextToken**

If present, this value indicates that more output is available than is included in the current response. Use this value in the `NextToken` request parameter in a subsequent call to the operation to get the next part of the output. You should repeat this until the `NextToken` response element comes back as `null`. This indicates that this is the last page of results.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

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

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**ThrottlingException**

Indicates that the principal has crossed the throttling limits of the API operations.

HTTP Status Code: 400

**ValidationException**

The request failed because it contains a syntax 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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

# PutConsoleAuthorizationConfiguration

Service: AWS Sign-In Control Plane

Enables AWS Management Console authorization configuration for an AWS account or organization. The operation automatically detects whether the `targetId` is an account ID or an organization ID, and applies the appropriate authorization scope.

## Request Syntax

```
{
   "targetId": "string"
}
```

## Request Parameters

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

The request accepts the following data in JSON format.

### targetId

The target identifier for the configuration. Accepts a 12-digit account ID, an organization ID (o-xxxxxxxxxx), or null/empty to use the caller's account ID. The scope is detected automatically based on the format.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 32.

Pattern: `(\d{12}|o-[a-z0-9]{10}|r-[0-9a-z]{4,32})`

Required: No

## Response Syntax

```
{
   "consoleAuthorizationEnabled": boolean,
   "scope": "string",
   "targetId": "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.

**consoleAuthorizationEnabled**

Indicates whether AWS Management Console authorization is enabled for the target.

Type: Boolean

**scope**

The scope that was applied to the configuration. Indicates whether the operation was applied at the account or organization level.

Type: String

**targetId**

The target identifier for which AWS Management Console authorization was configured.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 32.

Pattern: `(\d{12}|o-[a-z0-9]{10}|r-[0-9a-z]{4,32})`

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**ConflictException**

The request conflicts with the current state of the resource. For example, this exception is thrown when a client provides the same `ClientToken` for requests with differing parameter

values, or the same parameter values with different `ClientToken` within the expiration window.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**ResourceNotFoundException**

The request was denied because the specified resource was not found.

HTTP Status Code: 400

**TooManyRequestsError**

The request was denied due to rate limiting.

HTTP Status Code: 400

**ValidationException**

The request failed because it contains a syntax 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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

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

# PutResourcePermissionStatement

Service: AWS Sign-In Control Plane

Creates a permission statement in the account's AWS Sign-In resource-based policy that specifies under what conditions principals can access AWS resources. Conditions can scope access by source VPC, source VPC endpoint, source IP, or excluded principal.

## Request Syntax

```
{
   "clientToken": "string",
   "consoleSourceVpce": "string",
   "excludedPrincipal": "string",
   "requestedRegion": "string",
   "signinSourceVpce": "string",
   "sourceIp": "string",
   "sourceVpc": "string",
   "vpcSourceIp": "string"
}
```

## Request Parameters

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

The request accepts the following data in JSON format.

### clientToken

A unique, case-sensitive identifier that you provide to ensure the idempotency of the request. If not provided, the AWS SDK will automatically generate one for you.

Type: String

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

Pattern: `[!-~]+`

Required: No

### consoleSourceVpce

The AWS Management Console VPC endpoint identifier from which access is allowed. See `aws:SourceVpce` for more details.

Type: String

Pattern: `vpce-[a-z0-9]{8,20}`

Required: No

**excludedPrincipal**

The principal ARN that is excluded from policy evaluation. When a principal matching this ARN attempts to access an AWS resource, the resource-based policy is not evaluated.

Type: String

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

Pattern: `arn:aws:((iam::[0-9]{12}:role/[a-zA-Z0-9_+=,.@-]{1,64})|(iam::[0-9]{12}:user/[a-zA-Z0-9_+=,.@-]{1,64})|(sts::[0-9]{12}:federated-user/[a-zA-Z0-9_+=,.@-]{2,193})|(iam::[0-9]{12}:root))`

Required: No

**requestedRegion**

The AWS Region where the VPC resides. Required when `sourceVpc` is provided.

Type: String

Pattern: `[a-z]{2}(-[a-z]+)+-\d+`

Required: No

**signinSourceVpce**

The AWS Sign-In VPC endpoint identifier from which access is allowed. See `aws:SourceVpce` for more details.

Type: String

Pattern: `vpce-[a-z0-9]{8,20}`

Required: No

**sourceIp**

The IP address outside a VPC from which access is allowed. See `aws:SourceIp` for more details.

Type: String

Required: No

**sourceVpc**

The VPC identifier from which access is allowed. See `aws:SourceVpc` for more details.

Type: String

Pattern: `vpc-([0-9a-f]{8}|[0-9a-f]{17})`

Required: No

**vpcSourceIp**

The IP address in a VPC from which access is allowed. See `aws:VpcSourceIp` for more details.

Type: String

Required: No

## Response Syntax

```
{
   "statementId": "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.

**statementId**

The unique identifier of the created permission statement.

Type: String

Pattern: `[A-Za-z0-9+/]{64}=?`

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**ConflictException**

The request conflicts with the current state of the resource. For example, this exception is thrown when a client provides the same `ClientToken` for requests with differing parameter values, or the same parameter values with different `ClientToken` within the expiration window.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**ServiceQuotaExceededException**

The request would cause a service quota to be exceeded.

HTTP Status Code: 400

**TooManyRequestsError**

The request was denied due to rate limiting.

HTTP Status Code: 400

**ValidationException**

The request failed because it contains a syntax 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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

## AWS Sign-In Data Plane

The following actions are supported by AWS Sign-In Data Plane:

- AuthorizeOAuth2Access
- CreateOAuth2PublicClient
- CreateOAuth2Token
- CreateOAuth2TokenWithIAM
- IntrospectOAuth2TokenWithIAM
- RevokeOAuth2TokenWithIAM

# AuthorizeOAuth2Access

Service: AWS Sign-In Data Plane

Grants permission to authenticate through a browser and obtain an OAuth 2.0 authorization code for credential exchange.

## Request Syntax

```
GET /v1/authorize?
client_id=clientId&code_challenge=codeChallenge&code_challenge_method=codeChallengeMethod&redir
 HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### clientId

Client identifier which is unique to authorization server. Expected values: `arn:aws:signin:::devtools/same-device`, `arn:aws:signin:::devtools/cross-device`, or `arn:aws:signin:{region}::external-client/dcr/{uuid}` for dynamically registered clients.

Pattern: `arn:aws:signin:::devtools/(same-device|cross-device)$|^arn:aws:signin:[^:]*::external-client/dcr/.*`

Required: Yes

### codeChallenge

PKCE code challenge (SHA-256 hash of code verifier). Base64URL encoded, 43-128 characters.

Length Constraints: Minimum length of 43. Maximum length of 128.

Pattern: `[A-Za-z0-9\-._~]+`

Required: Yes

### codeChallengeMethod

PKCE code challenge method - must be `SHA-256` for AWS CLI.

Pattern: SHA-256

Required: Yes

**redirectUri**

Redirect URI where authorization code will be sent.

Same-device: `http://127.0.0.1:PORT/oauth/callback`

Cross-device: `https://{region}.signin.aws.amazon.com/v1/sessions/confirmation`

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

**resource**

The OAuth resource for which the access token is requested. This identifies the target service that the token grants access to. To scope the access token down to the specific resource, the resource parameter is mandated under RFC 8707 (Resource Indicators for OAuth 2.0).

If the client is a dynamically registered (DCR) client, this parameter is required.

Example: `https://aws-mcp.us-east-1.api.aws/mcp`.

Length Constraints: Minimum length of 1. Maximum length of 2048.

**responseType**

OAuth 2.0 response type - must be `code` for authorization code flow.

Pattern: `code`

Required: Yes

**scope**

OAuth 2.0 scope parameter - must be `openid` for AWS CLI clients.

Pattern: `openid`

**state**

CSRF protection parameter to prevent authorization injection attacks.

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

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 302
Location: location
```

## Response Elements

If the action is successful, the service sends back an HTTP 302 response.

The response returns the following HTTP headers.

**location**

HTTP Location header containing the redirect URI with authorization code and state parameters.

Response format: `{redirect_uri}?code={authorization_code}&state={state_parameter}`

Where:

- `redirect_uri`: The same URI provided in the authorization request
- `authorization_code`: A short-lived, single-use code for token exchange
- `state`: The same state value from the original request (CSRF protection)

Example values:

- `http://127.0.0.1:PORT/oauth/callback?code=ABC123&state=xyz`
- `https://{region}.signin.aws.amazon.com/v1/sessions/confirmation?code=DEF456&state=abc`

## Errors

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

**BadRequestException**

The request is invalid. Used for OAuth 2.0 request validation errors such as missing required parameters, invalid parameter values, malformed PKCE parameters, or invalid scope values.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**TooManyRequestsError**

Indicates that the principal has exceeded the limit of requests to this API operation.

HTTP Status Code: 429

## See Also

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

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

# CreateOAuth2PublicClient

Service: AWS Sign-In Data Plane

Dynamically registers an OAuth 2.0 public client for use with AWS Sign-In.

Implements RFC 7591 (OAuth 2.0 Dynamic Client Registration) for MCP-compatible agents. Only redirect URIs matching the allowlisted patterns are accepted during registration.

Registered clients receive an ARN in the format `arn:aws:signin:{region}::external-client/dcr/{uuid}`. Client registrations have a 90-day lifetime.

## Request Syntax

```
POST /v1/register HTTP/1.1
Content-type: application/json

{
   "grant_types": [ "string" ],
   "redirect_uris": [ "string" ],
   "response_types": [ "string" ],
   "token_endpoint_auth_method": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### grant_types

The grant types that this client will use. Supported values: `authorization_code`, `refresh_token`. Defaults to both if omitted. The `client_credentials` grant type is not supported. The `refresh_token` grant type cannot be specified alone without `authorization_code`.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 5 items.

Required: No

**redirect_uris**

The redirect URIs that this client will use for OAuth callbacks. Only redirect URIs matching the allowlisted patterns are accepted. Maximum of 10 URIs.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 10 items.

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

**response_types**

The response types that this client will use. Only `code` is supported. Defaults to `["code"]` if omitted.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 5 items.

Required: No

**token_endpoint_auth_method**

The client authentication method for the token endpoint. Only `none` is supported (public clients). Defaults to `none` if omitted.

Type: String

Pattern: `none`

Required: No

## Response Syntax

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

{
```

```
    "client_id": "string",
    "client_id_issued_at": number,
    "grant_types": [ "string" ],
    "redirect_uris": [ "string" ],
    "response_types": [ "string" ],
    "token_endpoint_auth_method": "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.

**client_id**

The unique client identifier (ARN) assigned to this client. Format: `arn:aws:signin:{region}::external-client/dcr/{uuid}`.

Type: String

**client_id_issued_at**

The time at which the client identifier was issued, as a NumericDate (Unix epoch seconds).

Type: Long

**grant_types**

The grant types registered for this client.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 5 items.

**redirect_uris**

The redirect URIs registered for this client.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 10 items.

Length Constraints: Minimum length of 1. Maximum length of 2048.

**response_types**

The response types registered for this client.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 5 items.

**token_endpoint_auth_method**

The client authentication method. Always none for public clients.

Type: String

Pattern: none

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**TooManyRequestsError**

Indicates that the principal has exceeded the limit of requests to this API operation.

HTTP Status Code: 429

**ValidationException**

The request failed because it contains a syntax 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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

# CreateOAuth2Token

Service: AWS Sign-In Data Plane

Exchanges an authorization code or refresh token for an OAuth 2.0 access token and refresh token.

This operation accepts `application/x-www-form-urlencoded` requests (RFC 6749 §4.1.3).

> **Important**
>
> AWS AWS CLI and AWS SDK clients use `application/json` as the content type and receive a camelCase response. The `accessToken` field is an object containing `accessKeyId`, `secretAccessKey`, and `sessionToken` rather than an opaque Bearer JWT string.

## Request Syntax

```
POST /v1/token HTTP/1.1
Content-type: application/json

{
   "client_id": "string",
   "code": "string",
   "code_verifier": "string",
   "grant_type": "string",
   "redirect_uri": "string",
   "refresh_token": "string",
   "resource": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### client_id

The OAuth 2.0 client identifier. Expected values: `arn:aws:signin:::devtools/same-device`, `arn:aws:signin:::devtools/cross-device`, or `arn:aws:signin:{region}::external-client/dcr/{uuid}` for dynamically registered clients.

Type: String

Pattern: `arn:aws:signin:::devtools/(same-device|cross-device)$|^arn:aws:signin:[^:]*::external-client/dcr/.*`

Required: Yes

### code

The authorization code received from the `/v1/authorize` endpoint. Required when `grant_type=authorization_code`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

### code_verifier

The PKCE code verifier that proves possession of the original code challenge. Required when `grant_type=authorization_code`.

Type: String

Length Constraints: Minimum length of 43. Maximum length of 128.

Pattern: `[A-Za-z0-9\-._~]+`

Required: No

### grant_type

The OAuth 2.0 grant type. Supported values:

- `authorization_code` — Exchange an authorization code for tokens.
- `refresh_token` — Use a refresh token to obtain a new access token.

Type: String

Pattern: `(authorization_code|refresh_token)`

Required: Yes

**redirect_uri**

The redirect URI that was used in the original authorization request. Must match exactly. Required when `grant_type=authorization_code`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

**refresh_token**

The refresh token issued by a previous token response. Required when `grant_type=refresh_token`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

**resource**

The OAuth resource for which the access token is requested (RFC 8707). Identifies the target service the token grants access to.

Required for dynamically registered (DCR) clients.

Example: `https://aws-mcp.us-east-1.api.aws/mcp`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

## Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "access_token": "string",
   "expires_in": number,
   "id_token": "string",
   "refresh_token": "string",
   "token_type": "string"
}
```

## Response Elements

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

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

**access_token**

The access token issued by the authorization server. This is an opaque Bearer JWT string (prefix AS0A). Use as a `Bearer` token in the `Authorization` header when calling the target resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

**expires_in**

The number of seconds until the access token expires. Maximum value is 900 seconds (15 minutes).

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 900.

**id_token**

A JSON Web Token (JWT) containing user identity claims. Present only when `grant_type=authorization_code`. Not included in refresh token responses.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

**refresh_token**

An encrypted refresh token that can be used to obtain new access tokens without re-authenticating. Valid for up to 12 hours.

Each time a refresh token is used, a new refresh token is returned (token rotation). Always use the most recently issued refresh token for subsequent requests.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

**token_type**

The type of token issued. Value is `Bearer` per RFC 6749 §5.1.

Type: String

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**TooManyRequestsError**

Indicates that the principal has exceeded the limit of requests to this API operation.

HTTP Status Code: 429

**ValidationException**

The request failed because it contains a syntax 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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

# CreateOAuth2TokenWithIAM

Service: AWS Sign-In Data Plane

Exchanges client credentials for an OAuth 2.0 access token scoped to a resource, which you can use to access AWS services from applications.

Implements the OAuth 2.0 client credentials grant. Applications authenticate to the token endpoint using SigV4 signing, and AWS Sign-In returns a short-lived OAuth access token (JWT) scoped to the requested resource.

The returned access token is a Bearer token per the OAuth 2.0 specification. The token is a JSON Web Token (JWT). Token lifetime is the minimum of the caller's session validity and 1 hour (3600 seconds).

## Request Syntax

```
POST /v1/token?x-amz-client-auth-method=iam HTTP/1.1
Content-type: application/json

{
   "grant_type": "string",
   "resource": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

**grant_type**

The OAuth 2.0 grant type. Must be `client_credentials`.

Type: String

Pattern: `client_credentials`

Required: Yes

**resource**

The OAuth resource for which the access token is requested. This identifies the target service that the token grants access to. To scope the access token down to the specific resource, the resource parameter is mandated under RFC 8707 (Resource Indicators for OAuth 2.0).

When using a dynamically registered client (DCR), the resource parameter is required.

Example: `aws-mcp.amazonaws.com`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

## Response Syntax

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

{
   "access_token": "string",
   "expires_in": number,
   "token_type": "string"
}
```

## Response Elements

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

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

**access_token**

JWT access token containing principal identity, resource scope, and session metadata. Use this token as a Bearer token when accessing the target resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

**expires_in**

Token lifetime in seconds. Value is the minimum of the caller's session validity and 1 hour (3600 seconds).

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 3600.

**token_type**

Always `Bearer` per OAuth 2.0 specification.

Type: String

Pattern: `Bearer`

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**TooManyRequestsError**

Indicates that the principal has exceeded the limit of requests to this API operation.

HTTP Status Code: 429

**ValidationException**

The request failed because it contains a syntax 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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

# IntrospectOAuth2TokenWithIAM

Service: AWS Sign-In Data Plane

Inspects the metadata and active state of an OAuth 2.0 access token or refresh token.

Implements RFC 7662 (OAuth 2.0 Token Introspection) over a SigV4-authenticated endpoint. Returns the claims associated with a token issued by AWS Sign-In. It inspects the metadata of a token issued by AWS Sign-In and returns the claims associated with it.

When the supplied token is unknown, expired, revoked, malformed, or owned by a different account, the response contains only `{"active": false}` with all other claims omitted.

## Request Syntax

```
POST /v1/introspect?x-amz-client-auth-method=iam HTTP/1.1
Content-type: application/json

{
   "token": "string",
   "token_type_hint": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### token

The string value of the token to introspect. Can be an access token or a refresh token issued by AWS Sign-In.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `ASO[AR][A-Za-z0-9+/=_\-]+`

Required: Yes

### token_type_hint

An optional hint about the type of the token submitted for introspection per RFC 7662. The server checks both token types regardless of the hint provided. Allowed values: `access_token`, `refresh_token`.

Type: String

Pattern: `(access_token|refresh_token)`

Required: No

## Response Syntax

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

{
   "account_id": "string",
   "active": boolean,
   "aud": "string",
   "client_id": "string",
   "exp": number,
   "iat": number,
   "iss": "string",
   "jti": "string",
   "nbf": number,
   "resource": "string",
   "signin_session": "string",
   "sub": "string",
   "token_type": "string",
   "user_id": "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.

### account_id

12-digit AWS account ID of the token's subject principal.

Type: String

Pattern: `[0-9]{12}`

**active**

Indicates whether the token is currently active. Returns `true` only when the token is valid, has not expired, has not been revoked, and belongs to the caller's account.

Type: Boolean

**aud**

Audience of the token: the OAuth resource the token is scoped to. Omitted for refresh tokens.

Type: String

**client_id**

Client identifier for the OAuth 2.0 client that requested the token.

Type: String

**exp**

Token expiration time as a NumericDate (Unix epoch seconds).

Type: Long

**iat**

Token issuance time as a NumericDate (Unix epoch seconds).

Type: Long

**iss**

Issuer of the token. Always `signin.amazonaws.com` for AWS Sign-In.

Type: String

**jti**

Unique identifier for the token.

Type: String

**nbf**

Token "not before" time as a NumericDate (Unix epoch seconds).

Type: Long

**resource**

The OAuth resource the token is scoped to. Only present for refresh token introspection.

Type: String

**signin_session**

AWS Sign-In session ARN bound to the token, of the form `arn:aws:signin:{region}:{account}:session/{uuid}`.

Type: String

**sub**

Subject of the token: the IAM principal Amazon Resource Name (ARN). For assumed-role sessions, this is the session ARN.

Type: String

**token_type**

Indicates which kind of token was introspected. One of `access_token` or `refresh_token`.

Type: String

Pattern: `(access_token|refresh_token)`

**user_id**

User identifier matching the `UserId` field from `sts:GetCallerIdentity` for the token's subject principal.

Type: String

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**TooManyRequestsError**

Indicates that the principal has exceeded the limit of requests to this API operation.

HTTP Status Code: 429

**ValidationException**

The request failed because it contains a syntax 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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

# RevokeOAuth2TokenWithIAM

Service: AWS Sign-In Data Plane

Revokes an OAuth 2.0 refresh token and its associated token chain.

Implements RFC 7009 (OAuth 2.0 Token Revocation) over a SigV4-authenticated endpoint. Invalidates the specified refresh token so that it can no longer be used to obtain new access tokens.

This operation is idempotent – revoking an already-revoked, expired, or otherwise invalid token returns 200 OK with an empty body. Only refresh tokens (prefix AS0R) are accepted.

> **Important**
>
> Revoking a refresh token does not invalidate access tokens that were previously issued using that refresh token. Existing access tokens remain valid until they expire (up to 1 hour). To immediately block access, use an IAM policy with `aws:SignInSessionArn` to deny the specific session.

## Request Syntax

```
POST /v1/revoke?x-amz-client-auth-method=iam HTTP/1.1
Content-type: application/json

{
   "token": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### token

The refresh token to revoke. Must be a refresh token issued by AWS Sign-In (prefix AS0R). Access tokens are not accepted for revocation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `ASOR[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 Error Types.

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**InternalServerException**

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

HTTP Status Code: 500

**TooManyRequestsError**

Indicates that the principal has exceeded the limit of requests to this API operation.

HTTP Status Code: 429

**ValidationException**

The request failed because it contains a syntax 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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

# Data Types

The following data types are supported by AWS Sign-In Control Plane:

- PermissionStatementSummary
- PolicyStatement
- SigninResourceBasedPolicy
- ValidationExceptionField

The following data types are supported by AWS Sign-In Data Plane:

- CreateOAuth2TokenRequestBody
- CreateOAuth2TokenResponseBody

# AWS Sign-In Control Plane

The following data types are supported by AWS Sign-In Control Plane:

- PermissionStatementSummary
- PolicyStatement
- SigninResourceBasedPolicy
- ValidationExceptionField

# PermissionStatementSummary

Service: AWS Sign-In Control Plane

Summary information for a permission statement in the AWS Sign-In resource-based policy.

## Contents

**sid**

The unique identifier of the permission statement.

Type: String

Pattern: `[A-Za-z0-9+/]{64}=?`

Required: Yes

**condition**

The condition block that defines under what conditions this statement applies.

Type: String to string to array of strings map map

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

# PolicyStatement

Service: AWS Sign-In Control Plane

An individual statement within the AWS Sign-In resource-based policy.

## Contents

**action**

The actions the statement controls.

Type: Array of strings

Required: No

**condition**

The condition block that scopes when the statement applies.

Type: String to string to array of strings map map

Required: No

**effect**

The effect of the statement, either `Allow` or `Deny`.

Type: String

Required: No

**principal**

The principal the statement applies to.

Type: String to string map

Required: No

**resource**

The resource the statement applies to.

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

# SigninResourceBasedPolicy

Service: AWS Sign-In Control Plane

The consolidated AWS Sign-In resource-based policy document for an account.

## Contents

**statement**

The list of statements in the policy.

Type: Array of PolicyStatement objects

Required: No

**version**

The version of the policy language.

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

## ValidationExceptionField

Service: AWS Sign-In Control Plane

Returns information about a field passed inside a request that resulted in an exception. For example, the request has failed because you passed an instance of IAM Identity Center without an organization.

### Contents

**message**

Message describing why the field failed validation.

Type: String

Required: Yes

**name**

The name of the field which failed the validation. For example, `NOT_ORG_BASED_INSTANCE`.

Type: String

Required: Yes

### See Also

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

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

# AWS Sign-In Data Plane

The following data types are supported by AWS Sign-In Data Plane:

- CreateOAuth2TokenRequestBody
- CreateOAuth2TokenResponseBody

# CreateOAuth2TokenRequestBody

Service: AWS Sign-In Data Plane

Input for the `CreateOAuth2Token` operation.

Supports both authorization code and refresh token flows. The flow is determined by the `grant_type` parameter. All field names use snake_case per RFC 6749.

## Contents

**client_id**

The OAuth 2.0 client identifier. Expected values: `arn:aws:signin:::devtools/same-device`, `arn:aws:signin:::devtools/cross-device`, or `arn:aws:signin:{region}::external-client/dcr/{uuid}` for dynamically registered clients.

Type: String

Pattern: `arn:aws:signin:::devtools/(same-device|cross-device)$|^arn:aws:signin:[^:]*::external-client/dcr/.*`

Required: Yes

**grant_type**

The OAuth 2.0 grant type. Supported values:

- `authorization_code` — Exchange an authorization code for tokens.
- `refresh_token` — Use a refresh token to obtain a new access token.

Type: String

Pattern: `(authorization_code|refresh_token)`

Required: Yes

**code**

The authorization code received from the `/v1/authorize` endpoint. Required when `grant_type=authorization_code`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

**code_verifier**

The PKCE code verifier that proves possession of the original code challenge. Required when `grant_type=authorization_code`.

Type: String

Length Constraints: Minimum length of 43. Maximum length of 128.

Pattern: `[A-Za-z0-9\-._~]+`

Required: No

**redirect_uri**

The redirect URI that was used in the original authorization request. Must match exactly. Required when `grant_type=authorization_code`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

**refresh_token**

The refresh token issued by a previous token response. Required when `grant_type=refresh_token`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

**resource**

The OAuth resource for which the access token is requested (RFC 8707). Identifies the target service the token grants access to.

Required for dynamically registered (DCR) clients.

Example: `https://aws-mcp.us-east-1.api.aws/mcp`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

## See Also

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

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

# CreateOAuth2TokenResponseBody

Service: AWS Sign-In Data Plane

Response from the `CreateOAuth2Token` operation following RFC 6749 §5.1.

> **Note**
>
> AWS AWS CLI and AWS SDK clients use `application/json` as the content type and receive a camelCase response. The `accessToken` field is an object containing `accessKeyId`, `secretAccessKey`, and `sessionToken` rather than an opaque Bearer JWT string.

## Contents

**access_token**

The access token issued by the authorization server. This is an opaque Bearer JWT string (prefix AS0A). Use as a `Bearer` token in the `Authorization` header when calling the target resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Required: Yes

**expires_in**

The number of seconds until the access token expires. Maximum value is 900 seconds (15 minutes).

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 900.

Required: Yes

**refresh_token**

An encrypted refresh token that can be used to obtain new access tokens without re-authenticating. Valid for up to 12 hours.

Each time a refresh token is used, a new refresh token is returned (token rotation). Always use the most recently issued refresh token for subsequent requests.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

**token_type**

The type of token issued. Value is `Bearer` per RFC 6749 §5.1.

Type: String

Required: Yes

**id_token**

A JSON Web Token (JWT) containing user identity claims. Present only when `grant_type=authorization_code`. Not included in refresh token responses.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Required: No

## See Also

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

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

# Common Parameters

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

**X-Amz-Algorithm**

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

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

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

**X-Amz-Credential**

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

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

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

Type: string

Required: Conditional

**X-Amz-Date**

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

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

Type: string

Required: Conditional

**X-Amz-Security-Token**

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

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

Type: string

Required: Conditional

**X-Amz-Signature**

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

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

Type: string

Required: Conditional

**X-Amz-SignedHeaders**

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

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

Type: string

Required: Conditional

# Common Error Types

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

**AccessDeniedException**

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

HTTP Status Code: 403

**ExpiredTokenException**

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

HTTP Status Code: 403

**IncompleteSignature**

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

HTTP Status Code: 403

**InternalFailure**

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

HTTP Status Code: 500

**MalformedHttpRequestException**

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

HTTP Status Code: 400

**NotAuthorized**

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

HTTP Status Code: 401

**OptInRequired**

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

HTTP Status Code: 403

**RequestAbortedException**

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

HTTP Status Code: 400

**RequestEntityTooLargeException**

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

HTTP Status Code: 413

**RequestTimeoutException**

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

HTTP Status Code: 408

**ServiceUnavailable**

The service is temporarily unavailable. Try again later.

HTTP Status Code: 503

**ThrottlingException**

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

HTTP Status Code: 400

**UnknownOperationException**

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

HTTP Status Code: 404

**UnrecognizedClientException**

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

HTTP Status Code: 403

**ValidationError**

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

HTTP Status Code: 400