IAM 5.0 API Reference

Issue 01

Date 2025-12-03

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Before You Start

Welcome to Identity and Access Management (IAM). IAM provides identity authentication, permissions management, and access control. With IAM, you can create and manage users and grant them permissions to allow or deny their access to cloud resources.

IAM supports the console access and programmatic access (API access). This document describes how to use APIs to perform operations on IAM, such as creating users and user groups. Before calling IAM APIs, ensure that you have understood the basic concepts of this service. For details, see the *Identity and Access Management Service Overview*.

Basic Concepts

- Account

  An account is created upon successful registration with Huawei Cloud. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity and should not be used directly to perform routine management. For security purposes, create IAM users and grant them permissions for routine management.

- IAM user

  An IAM user is created using an account to use cloud services. Each IAM user has their own identity credentials (password and access keys).

  An IAM user can view the account ID and IAM user ID on the page of the console.

- Region

  Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.

- AZ

  An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an

AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected by optical fibers for high-availability networking.

2 API Overview

Type	API	Description
Management plane	IAM User Management	Used to create, query, modify, and delete an IAM user.
	Credential Management	Used to create, query, modify, and delete a permanent access key or user login information.
	Virtual MFA Device Management	Used to enable, disable, create, query, and delete a virtual MFA device.
	Security Settings	Used to query and modify the password policy and login policy of an account.
	User Group Management	Used to create, query, modify, and delete a user group, and add a user to or remove a user from a specified user group.
	Identity Policy Management	Used to create, query, and delete an identity policy.
	Identity Policy Version Management	Used to create, query, modify, and delete an identity policy version.
	Permissions Management	Used to attach an identity policy to or detach an identity policy from an identity, and query an identity policy.
	Service-linked Agency Management	Used to create, query, and delete a service-linked agency.
	Service Principal Query	Used to obtain all service principals.

Type	API	Description
	Authorization Summary Query	Used to query the authorization summary of a specified service and the list of registered cloud services.
	Agency and Trust Agency Management	Used to create, query, modify, and delete an agency or trust agency.
	Account Summary Query	Used to obtain summary information about the IAM principal usage and IAM quota of an account.
	Account Function Query	Used to obtain the function status of an account.
	Resource Tag Management	Used to create, query, and delete tags for IAM resources.
	Asymmetric Signature Management	Used to enable or disable the asymmetric signature for a tenant, and obtain the asymmetric signature status of a tenant.
Temporary security credential	Obtaining a Temporary Access Key Through an Agency or Trust Agency	Used to obtain a temporary access key through an agency or trust agency. The temporary access key can be used to control access to cloud resources.
	Obtaining the Identity Information of a Caller	Used to obtain the identity information of a caller (such as a user or agency).
	Decoding the Authentication Failure Cause	Used to decode the authentication failure cause.

3 Calling APIs

3.1 Making an API Request

This section describes the structure of a REST API request and use the API for **obtaining a temporary security credential through an agency or trust agency** as an example to describe how to call an API. By using the API, a temporary security credential is obtained through an agency or trust agency. The obtained security credential contains the user identity information and permissions and is used to sign the requests for other API calls.

Request URI

A request URI is in the following format:

{URI-scheme}://{Endpoint}/{resource-path}?{query-string}

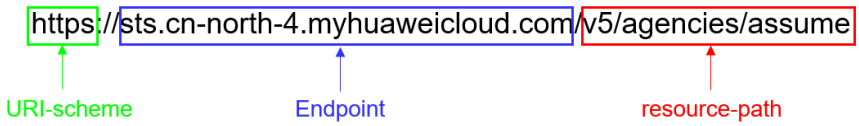
Although a request URI is included in the request header, most programming languages or frameworks require the request URI to be transmitted separately.

- **URI-scheme**: Protocol used to transmit requests. All APIs use **HTTPS**.
- **Endpoint**: Domain name or IP address of the server running the REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints**. .
- **resource-path**: Access path of an API for performing a specified operation. It can be obtained from the URI of an API. For example, the **resource-path** of the API used to obtain a temporary security credential through an agency or trust agency is **/v5/agencies/assume**.
- **query-string**: Query parameter, which is optional for APIs. Ensure that a question mark (**?**) is included before each query parameter that is in the format of **Parameter name=Parameter value**. For example, **limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to obtain a temporary security credential in the **CN North-Beijing4** region, obtain the endpoint of IAM (**sts.cn-north-4.myhuaweicloud.com**) for this region and the **resource-path** (**/v5/agencies/assume**) in the URI of the API for **obtaining a temporary security credential through an agency or trust agency**. Then, construct the URI as follows:


```
https://sts.cn-north-4.myhuaweicloud.com/v5/agencies/assume
```

Figure 3-1 Example URI



NOTE

To simplify the URI display in this document, each API is provided only with a **resource-path** and a request method. The **URI-scheme** of all APIs is **HTTPS**, and the endpoints of all APIs in the same region are identical.

Request Methods

The HTTP protocol defines the following request methods that can be used to send a request to the server:

- **GET**: requests the server to return specified resources.
- **PUT**: requests the server to update specified resources.
- **POST**: requests the server to add resources or perform special operations.
- **DELETE**: requests the server to delete specified resources, for example, an object.
- **HEAD**: requests the server to return only the response header.
- **PATCH**: requests the server to update partial content of a specified resource. If the resource does not exist, a new resource will be created.

For example, in the URI of the API for **obtaining a temporary security credential through an agency or trust agency**, the request method is **POST** and the request is as follows:

```
POST https://sts.cn-north-4.myhuaweicloud.com/v5/agencies/assume
```

Request Header

You can also add additional header fields to a request, such as the fields required by a specified URI or HTTP method. For example, to request for the authentication information, add **Content-Type**, which specifies the request body type.

Common request header fields are as follows:

- **Content-Type**: specifies the request body type or format. This field is mandatory and its default value is **application/json**. Other values of this field will be provided for specific APIs if any.
- **Authorization**: requests signature information. This field is mandatory. You can use a permanent AK/SK pair or temporary security credential to sign requests based on **AK/SK-based Authentication**.

> **NOTE**
>
> APIs support AK/SK authentication, which uses SDKs to sign a request. During the signature, the **Authorization** (signature information) and **X-Sdk-Date** (time when the request is sent) headers are automatically added in the request.
>
> For more information, see **AK/SK-based Authentication**.

- **X-Project-ID**: subproject ID. This field is optional and can be used in multi-project scenarios.
- **X-Domain-ID**: account ID (equivalent to **AccountId**).

For the API used to **obtain a temporary security credential through an agency or trust agency**, an example of such requests is as follows:

```
POST https://sts.cn-north-4.myhuaweicloud.com/v5/agencies/assume
Content-Type: application/json
x-sdk-date: 20191115T033655Z
Authorization: SDK-HMAC-SHA256 Access=QTWAOYTTINDUT2QVKYUC, SignedHeaders=content-type;host;x-sdk-date, Signature=7be6668032f70418fcc22abc52071e57aff61b84a1d2381bb430d6870f4f6ebe
```

Request Body

The body of a request is often sent in a structured format as specified in the **Content-Type** header field. The request body transfers content except the request header. If the request body contains Chinese characters, these characters must be encoded in UTF-8.

For details about the message body of each API, see the API definition. Not all requests require a message body. For example, some GET and DELETE operations do not require a message body.

For the API used to **obtain a temporary security credential through an agency or trust agency**, you can obtain the request parameters and parameter descriptions from the API request. The following provides an example request with a body included. Replace ***agency_urn*** and ***agency_session_name*** with the actual values.

> **NOTE**
>
> The **duration_seconds** parameter specifies the validity period of a security credential. The security credential obtained in the following example is valid only for one hour. You can further define the permissions of security credentials. For details, see **Obtaining a Temporary Security Credential Through an Agency or Trust Agency**.

```
POST https://sts.cn-north-4.myhuaweicloud.com/v5/agencies/assume
Content-Type: application/json
x-sdk-date: xxxxxxxxxxxxxxxxx
Authorization: ********

{
  "duration_seconds": "3600"
  "agency_urn": "agency_urn",
  "agency_session_name": "agency_session_name",
}
```

If all data required for the API request is available, you can send the request to call the API through **curl**, **Postman**, or coding. In the response header for the API used to **obtain a temporary security credential through an agency or trust agency**, **credentials** is the desired temporary security credential. This temporary security credential can then be used to call other APIs through AK/SK-based authentication.

3.2 Authentication

Requests for calling an API can be authenticated only using the following method:

- AK/SK-based authentication: Requests are authenticated by encrypting the request body using an AK/SK pair.

AK/SK-based Authentication

NOTE

The AK/SK can be either a permanent access key or a temporary access key. If it is a temporary access key, the HTTP request header **X-Security-Token** must be contained.

AK/SK-based authentication supports API requests with a body not larger than 12 MB.

In AK/SK-based authentication, AK/SK is used to sign requests and the signature is then added to the requests for authentication.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

In AK/SK-based authentication, you can use an AK/SK to sign requests based on the signature algorithm or use the signing SDK to sign requests.

NOTICE

The signing SDK is only used for signing requests and is different from the SDKs provided by services.

3.3 Response

Status Code

After sending a request, you will receive a response, including a status code, response header, and response body.

Status code is a group of digits ranging from 1*xx* to 5*xx*. It indicates the status of a response. For more information, see **7.1 Status Codes**.

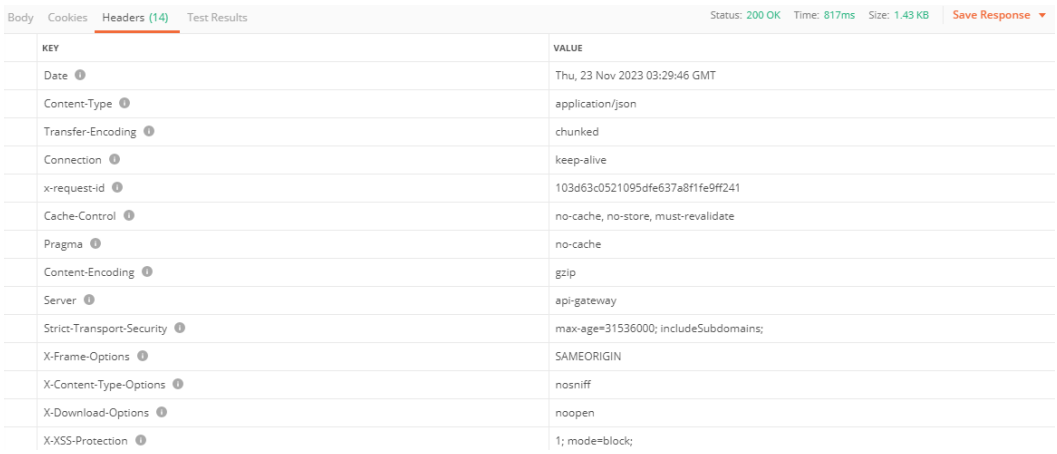
For example, if status code **200** is returned for calling the API used to **obtain a temporary security credential through an agency or trust agency**, the request is successful.

Response Header

Similar to a request, a response also has a header, for example, **Content-type**.

For the API used to **obtain a temporary security credential through an agency or trust agency**, **Figure 3-2** is the desired response header.

Figure 3-2 Response header for obtaining a temporary security credential through an agency or trust agency



Response Body

The body of a response is often returned in structured format as specified in the **Content-Type** header field. The response body transfers content except the response header.

The following is part of the response body for the API used to **obtain a temporary security credential through an agency or trust agency**.

```
{
   "source_identity": "{source_identity}",
   "assumed_agency": {
      "urn": "sts::{account_id}::assumed-agency:{agency_name}/{agency_session_name}",
      "id": "{agency_id}:{agency_session_name}"
   },
   "credentials": {
   "access_key_id":"HSTANOXZU2UXBS55JLJ3",
   "secret_access_key":"EoWCQrr...SCcw4Whkt2aXKWAr",
   "security_token":"hQpjbi1XXXXXX...XXXXXbhBbA0TQ==",
   "expiration":"2022-09-07T03:27:51.158Z"
   }
}
```

If an error occurs during API calling, an error code and error message will be displayed. The following example is an error response body:

```
{
   "error_code": "STS5.1106",
   "error_msg": "the agency 'iam::{account_id}:agency:{agency_name}' cannot be found"
}
```

In the response body, **error_code** is an error code, and **error_msg** provides information about the error.

4 API

4.1 IAM

4.1.1 Managing IAM Users

4.1.1.1 Listing IAM Users

Function

This API is used to list IAM users.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:listUsersV5	List	user *	-	-	-

URI

GET /v5/users

Table 4-1 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The value ranges from 1 to 200. The default value is 100. Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Pagination marker. The value contains 4 to 400 characters, including only letters, digits, and the following special characters: +/=-_ Minimum: **4** Maximum: **400**
group_id	No	String	Group ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

None

Response Parameters

Status code: 200

Table 4-2 Response body parameters

Parameter	Type	Description
users	Array of **User** objects	IAM user list.
page_info	**PageInfo** object	Pagination information.

Table 4-3 User

Parameter	Type	Description
description	String	IAM user description. The value can contain 0 to 255 characters and cannot contain the following special characters: @, #, %, &, <, >, \, $, ^, and *.
user_name	String	IAM username. The value contains 1 to 64 characters, including only letters, digits, underscores (_), hyphens (-), periods (.), and spaces, and cannot start with a digit.
is_root_user	Boolean	Indicates whether an IAM user is a root user.
created_at	String	Time when an IAM user was created.
user_id	String	IAM user ID.
urn	String	Uniform resource name.
enabled	Boolean	Indicates whether an IAM user is enabled.

Table 4-4 PageInfo

Parameter	Type	Description
next_marker	String	If this parameter exists, there are subsequent items that are not displayed in the current response body. The value can be used as the pagination marker parameter for the next request to obtain information about the next page. This API can be repeatedly called until this field does not exist.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-5 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 403

Table 4-6 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Example Requests

- Listing all users

  ```
  GET https://{endpoint}/v5/users
  ```

- Listing all users in group *xxx*

  ```
  GET https://{endpoint}/v5/users?group_id=xxx
  ```

Example Responses

Status code: 200

Successful

```
{
  "users" : [ {
    "description" : "description",
    "user_name" : "name",
    "is_root_user" : false,
    "created_at" : "2023-04-26T03:49:42Z",
    "user_id" : "string",
    "urn" : "iam::accountid:user:name",
    "enabled" : true
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```


Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden

Error Codes

See **Error Codes**.

4.1.1.2 Creating an IAM User

Function

This API is used to create an IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:createUserV5	Write	user *	-	-	-

URI

POST /v5/users

Request Parameters

Table 4-7 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	IAM username. The value contains 1 to 64 characters, including only letters, digits, underscores (_), hyphens (-), periods (.), and spaces, and cannot start with a digit.
description	No	String	IAM user description. The value can contain 0 to 255 characters and cannot contain the following special characters: @, #, %, &, <, >, \, $, ^, and *.
enabled	Yes	Boolean	Indicates whether an IAM user is enabled.

Response Parameters

Status code: 201

Table 4-8 Response body parameters

Parameter	Type	Description
user	**User** object	IAM user.

Table 4-9 User

Parameter	Type	Description
description	String	IAM user description. The value can contain 0 to 255 characters and cannot contain the following special characters: @, #, %, &, <, >, \, $, ^, and *.
user_name	String	IAM username. The value contains 1 to 64 characters, including only letters, digits, underscores (_), hyphens (-), periods (.), and spaces, and cannot start with a digit.

Parameter	Type	Description
is_root_user	Boolean	Indicates whether an IAM user is a root user.
created_at	String	Time when an IAM user was created.
user_id	String	IAM user ID.
urn	String	Uniform resource name.
enabled	Boolean	Indicates whether an IAM user is enabled.

Status code: 400

Table 4-10 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-11 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 409

Table 4-12 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Parameter	Type	Description
request_id	String	Request ID.

Example Requests

Creating an IAM user **name**

```
POST https://{endpoint}/v5/users

{
  "name" : "name",
  "description" : "description",
  "enabled" : true
}
```

Example Responses

Status code: 201

Successful

```
{
  "user" : {
    "description" : "description",
    "user_name" : "name",
    "is_root_user" : false,
    "created_at" : "2023-04-26T03:49:42Z",
    "user_id" : "string",
    "urn" : "iam::accountid:user:name",
    "enabled" : true
  }
}
```

Status Codes

Status Code	Description
201	Successful
400	Bad request
403	Forbidden
409	Conflict

Error Codes

See **Error Codes**.

4.1.1.3 Querying the Last Login Time of an IAM User

Function

This API is used to query the last login time of an IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:showUserLastLoginV5	Read	user *	g:ResourceTag/<tag-key>	-	-

URI

GET /v5/users/{user_id}/last-login

Table 4-13 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-14 Response body parameters

Parameter	Type	Description
user_last_login	**UserLastLogin** object	Last login time of an IAM user.

Table 4-15 UserLastLogin

Parameter	Type	Description
last_login_at	String	Last login time of an IAM user. If the value is **null**, the user has never logged in.

Status code: 403

Table 4-16 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-17 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying the last login time of an IAM user

```
GET https://{endpoint}/v5/users/{user_id}/last-login
```

Example Responses

Status code: 200

Successful

```
{
  "user_last_login" : {
    "last_login_at" : "2023-09-13T03:32:02.563Z"
```

```
  }
}
```

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.1.4 Querying IAM User Details

Function

This API is used to query IAM user details.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:getUserV5	Read	user *	g:ResourceTag/<tag-key>	-	-

URI

GET /v5/users/{user_id}

Table 4-18 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-19 Response body parameters

Parameter	Type	Description
user	**UserEx** object	IAM user.

Table 4-20 UserEx

Parameter	Type	Description
description	String	IAM user description. The value can contain 0 to 255 characters and cannot contain the following special characters: @, #, %, &, <, >, \, $, ^, and *.
user_name	String	IAM username. The value contains 1 to 64 characters, including only letters, digits, underscores (_), hyphens (-), periods (.), and spaces, and cannot start with a digit.
is_root_user	Boolean	Indicates whether an IAM user is a root user.
created_at	String	Time when an IAM user was created.
user_id	String	IAM user ID.
urn	String	Uniform resource name.
enabled	Boolean	Indicates whether an IAM user is enabled.
tags	Array of **Tag** objects	List of custom tags.

Table 4-21 Tag

Parameter	Type	Description
tag_key	String	Tag key. The value can contain 1 to 64 characters. Letters, digits, spaces, and the following special characters are allowed: _.:=+-@. The key cannot start with a space or _**sys**_ or end with a space. Minimum: **1** Maximum: **64**
tag_value	String	Tag value. The value can be an empty string or contain 0 to 128 characters. Letters, digits, spaces, and the following special characters are allowed: _.:/=+-@ Minimum: **0** Maximum: **128**

Status code: 403

Table 4-22 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-23 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying IAM user details

```
GET https://{endpoint}/v5/users/{user_id}
```

Example Responses

Status code: 200

Successful

```
{
  "user" : {
    "description" : "description",
    "user_name" : "name",
    "is_root_user" : false,
    "created_at" : "2023-04-26T03:49:42Z",
    "user_id" : "string",
    "urn" : "iam::accountid:user:name",
    "enabled" : true,
    "tags" : [ {
      "tag_key" : "key",
      "tag_value" : "value"
    } ]
  }
}
```

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.1.5 Modifying an IAM User

Function

This API is used to modify an IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:updateUserV5	Write	user *	g:ResourceTag/<tag-key>	-	-

URI

PUT /v5/users/{user_id}

Table 4-24 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Request Parameters

Table 4-25 Request body parameters

Parameter	Mandatory	Type	Description
new_user_name	No	String	IAM username. The value contains 1 to 64 characters, including only letters, digits, underscores (_), hyphens (-), periods (.), and spaces, and cannot start with a digit.
new_description	No	String	IAM user description. The value can contain 0 to 255 characters and cannot contain the following special characters: @, #, %, &, <, >, \, $, ^, and *.
enabled	No	Boolean	Indicates whether an IAM user is enabled.

Response Parameters

Status code: 200

Table 4-26 Response body parameters

Parameter	Type	Description
user	**User** object	IAM user.

Table 4-27 User

Parameter	Type	Description
description	String	IAM user description. The value can contain 0 to 255 characters and cannot contain the following special characters: @, #, %, &, <, >, \, $, ^, and *.
user_name	String	IAM username. The value contains 1 to 64 characters, including only letters, digits, underscores (_), hyphens (-), periods (.), and spaces, and cannot start with a digit.
is_root_user	Boolean	Indicates whether an IAM user is a root user.
created_at	String	Time when an IAM user was created.
user_id	String	IAM user ID.
urn	String	Uniform resource name.
enabled	Boolean	Indicates whether an IAM user is enabled.

Status code: 400

Table 4-28 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-29 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-30 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-31 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Modifying an IAM user

```
PUT https://{endpoint}/v5/users/{user_id}

{
  "new_user_name" : "name",
  "new_description" : "description",
  "enabled" : true
}
```

Example Responses

Status code: 200

Successful

```
{
  "user" : {
    "description" : "description",
    "user_name" : "name",
    "is_root_user" : false,
    "created_at" : "2023-04-26T03:49:42Z",
    "user_id" : "string",
    "urn" : "iam::accountid:user:name",
    "enabled" : true
  }
}
```

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.1.6 Deleting an IAM User

Function

This API is used to delete a specified IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:deleteUserV5	Write	user *	g:ResourceTag/<tag-key>	-	-

URI

DELETE /v5/users/{user_id}

Table 4-32 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Request Parameters

None

Response Parameters

Status code: 204

Successful

Status code: 403

Table 4-33 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-34 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-35 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Deleting a specified IAM user

```
DELETE https://{endpoint}/v5/users/{user_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.2 Managing Credentials

4.1.2.1 Querying the Last Usage Time of a Specified Permanent Access Key

Function

This API is used to query the last usage time of a specified permanent access key of an IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:credentials:showAccessKeyLastUsedV5	Read	user *	g:ResourceTag/<tag-key>	-	-

URI

GET /v5/users/{user_id}/access-keys/{access_key_id}/last-used

Table 4-36 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.
access_key_id	Yes	String	Permanent access key ID (AK). Minimum: **1** Maximum: **40**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-37 Response body parameters

Parameter	Type	Description
access_key_last_used	**AccessKeyLastUsed** object	Last usage time of the access key.

Table 4-38 AccessKeyLastUsed

Parameter	Type	Description
last_used_at	String	Last usage time of the access key. If no, the access key has never been used.

Status code: 403

Table 4-39 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-40 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying the last usage time of a specified permanent access key of an IAM user

```
GET https://{endpoint}/v5/users/{user_id}/access-keys/{access_key_id}/last-used
```

Example Responses

Status code: 200

Successful

```
{
  "access_key_last_used" : {
    "last_used_at" : "2023-09-13T06:51:20.550Z"
  }
}
```

Status Codes

Status Code	Description
200	Successful

Status Code	Description
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.2.2 Modifying a Specified Permanent Access Key

Function

This API is used to modify a specified permanent access key of an IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:credentials:updateCredentialV5	Write	user *	g:ResourceTag/<tag-key>	-	-

URI

PUT /v5/users/{user_id}/access-keys/{access_key_id}

Table 4-41 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.
access_key_id	Yes	String	Permanent access key ID (AK). Minimum: **1** Maximum: **40**

Request Parameters

Table 4-42 Request body parameters

Parameter	Mandatory	Type	Description
status	Yes	String	Status of the access key. The value can be active or inactive.

Response Parameters

Status code: 200

Table 4-43 Response body parameters

Parameter	Type	Description
access_key	**AccessKeyMetadata** object	Permanent access key.

Table 4-44 AccessKeyMetadata

Parameter	Type	Description
user_id	String	IAM user ID.
access_key_id	String	Permanent access key ID (AK).
created_at	String	Time when the access key was created.
status	String	Status of the access key. The value can be active or inactive.

Status code: 403

Table 4-45 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-46 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Setting the status of a specified permanent access key of an IAM user to **Enabled**

```
PUT https://{endpoint}/v5/users/{user_id}/access-keys/{access_key_id}

{
  "status" : "active"
}
```

Example Responses

Status code: 200

Successful

```
{
  "access_key" : {
    "user_id" : "user",
    "access_key_id" : "access",
    "created_at" : "2023-09-13T06:51:20.550Z",
    "status" : "active"
  }
}
```

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.2.3 Deleting a Specified Permanent Access Key

Function

This API is used to delete a specified permanent access key of an IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:credentials:deleteCredentialV5	Write	user *	g:ResourceTag/<tag-key>	-	-

URI

DELETE /v5/users/{user_id}/access-keys/{access_key_id}

Table 4-47 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.
access_key_id	Yes	String	Permanent access key ID (AK). Minimum: **1** Maximum: **40**

Request Parameters

None

Response Parameters

Status code: 204

Successful

Status code: 403

Table 4-48 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-49 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Deleting a specified permanent access key of an IAM user

```
DELETE https://{endpoint}/v5/users/{user_id}/access-keys/{access_key_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.2.4 Querying All Permanent Access Keys

Function

This API is used to query all permanent access keys of an IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:credentials:listCredentialsV5	List	user *	g:ResourceTag/<tag-key>	-	-

URI

GET /v5/users/{user_id}/access-keys

Table 4-50 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Table 4-51 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The value ranges from 1 to 200. The default value is 100. Minimum: **1** Maximum: **200** Default: **100**

Parameter	Mandatory	Type	Description
marker	No	String	Pagination marker. The value contains 4 to 400 characters, including only letters, digits, and the following special characters: +/=-_ Minimum: **4** Maximum: **400**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-52 Response body parameters

Parameter	Type	Description
access_keys	Array of **AccessKeyMetadata** objects	List of permanent access keys.
page_info	**PageInfo** object	Pagination information.

Table 4-53 AccessKeyMetadata

Parameter	Type	Description
user_id	String	IAM user ID.
access_key_id	String	Permanent access key ID (AK).
created_at	String	Time when the access key was created.
status	String	Status of the access key. The value can be active or inactive.

Table 4-54 PageInfo

Parameter	Type	Description
next_marker	String	If this parameter exists, there are subsequent items that are not displayed in the current response body. The value can be used as the pagination marker parameter for the next request to obtain information about the next page. This API can be repeatedly called until this field does not exist.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-55 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-56 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-57 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying all permanent access keys of an IAM user

```
GET https://{endpoint}/v5/users/{user_id}/access-keys
```

Example Responses

Status code: 200

Successful

```
{
  "access_keys" : [ {
    "user_id" : "user",
    "access_key_id" : "access",
    "created_at" : "2023-09-13T06:51:20.550Z",
    "status" : "active"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.2.5 Creating a Permanent Access Key

Function

This API is used to create a permanent access key for an IAM user.

AKs or SKs are identity credentials for using development tools (API, CLI, and SDK) to access resources and cannot be used for console login. AK is a unique identifier used in conjunction with SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:credentials:createCredentialV5	Write	user *	g:ResourceTag/<tag-key>	-	-

URI

POST /v5/users/{user_id}/access-keys

Table 4-58 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Request Parameters

None

Response Parameters

Status code: 201

Table 4-59 Response body parameters

Parameter	Type	Description
access_key	**AccessKey** object	Created permanent access key.

Table 4-60 AccessKey

Parameter	Type	Description
user_id	String	IAM user ID.
access_key_id	String	ID of the created permanent access key (AK).
created_at	String	Time when the access key was created.
secret_access_key	String	Created SK.
status	String	Status of the access key. The value can be active or inactive.

Status code: 400

Table 4-61 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-62 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-63 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Creating a permanent access key for an IAM user

```
POST https://{endpoint}/v5/users/{user_id}/access-keys
```

Example Responses

Status code: 201

Successful

```
{
  "access_key" : {
    "user_id" : "user",
    "access_key_id" : "access",
    "created_at" : "2023-09-13T06:51:20.550Z",
    "secret_access_key" : "secret",
    "status" : "active"
  }
}
```

Status Codes

Status Code	Description
201	Successful
400	Bad request
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.2.6 Changing the Login Password of an IAM User

Function

This API is used to change the login password of an IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:changePasswordV5	Write	user *	g:ResourceTag/<tag-key>	-	-

URI

POST /v5/caller-password

Request Parameters

Table 4-64 Request body parameters

Parameter	Mandatory	Type	Description
new_password	Yes	String	New password of an IAM user.
old_password	Yes	String	Old password of an IAM user.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-65 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-66 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-67 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Changing the login password of an IAM user. The old password is **Password1**, and the new password is **Password2**.

```
POST https://{endpoint}/v5/caller-password

{
  "new_password" : "Password2",
  "old_password" : "Password1"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden

Status Code	Description
404	Not found

Error Codes

See **Error Codes**.

4.1.2.7 Querying the Login Information of an IAM User

Function

This API is used to query the login information of a specified IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:showLoginProfileV5	Read	user *	g:ResourceTag/<tag-key>	-	-

URI

GET /v5/users/{user_id}/login-profile

Table 4-68 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-69 Response body parameters

Parameter	Type	Description
login_profile	**LoginProfile** object	IAM user login information.

Table 4-70 LoginProfile

Parameter	Type	Description
user_id	String	IAM user ID.
password_reset_required	Boolean	Indicates whether an IAM user needs to change their password upon the next login.
password_expires_at	String	Time when the password of an IAM user expires.
created_at	String	Time when the IAM user login information was created.

Status code: 403

Table 4-71 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-72 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying the login information of a specified IAM user

```
GET https://{endpoint}/v5/users/{user_id}/login-profile
```

Example Responses

Status code: 200

Successful

```
{
  "login_profile" : {
    "user_id" : "user",
    "password_reset_required" : true,
    "password_expires_at" : "2023-09-13T08:03:10.781Z",
    "created_at" : "2023-09-13T08:03:10.781Z"
  }
}
```

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.2.8 Creating the Login Information of an IAM User

Function

This API is used to create the login information of a specified IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:createLoginProfileV5	Write	user *	g:ResourceTag/<tag-key>	-	-

URI

POST /v5/users/{user_id}/login-profile

Table 4-73 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Request Parameters

Table 4-74 Request body parameters

Parameter	Mandatory	Type	Description
password	Yes	String	IAM user password.
password_reset_required	Yes	Boolean	Indicates whether an IAM user needs to change their password upon the next login.

Response Parameters

Status code: 201

Table 4-75 Response body parameters

Parameter	Type	Description
login_profile	**LoginProfile** object	IAM user login information.

Table 4-76 LoginProfile

Parameter	Type	Description
user_id	String	IAM user ID.
password_reset_required	Boolean	Indicates whether an IAM user needs to change their password upon the next login.
password_expires_at	String	Time when the password of an IAM user expires.
created_at	String	Time when the IAM user login information was created.

Status code: 400

Table 4-77 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-78 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-79 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-80 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Creating the login information of a specified IAM user. The password is set to **Password0** and the user is asked to change the password upon the next login.

```
POST https://{endpoint}/v5/users/{user_id}/login-profile

{
  "password" : "Password0",
  "password_reset_required" : true
}
```

Example Responses

Status code: 201

Successful

```
{
  "login_profile" : {
    "user_id" : "user",
    "password_reset_required" : true,
    "password_expires_at" : "2023-09-13T08:03:10.781Z",
    "created_at" : "2023-09-13T08:03:10.781Z"
  }
}
```

Status Codes

Status Code	Description
201	Successful
400	Bad request
403	Forbidden

Status Code	Description
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.2.9 Modifying the Login Information of an IAM User

Function

This API is used to modify the login information of a specified IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:updateLoginProfileV5	Write	user *	g:ResourceTag/<tag-key>	-	-

URI

PUT /v5/users/{user_id}/login-profile

Table 4-81 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Request Parameters

Table 4-82 Request body parameters

Parameter	Mandatory	Type	Description
password	No	String	IAM user password.
password_reset_required	No	Boolean	Indicates whether an IAM user needs to change their password upon the next login.

Response Parameters

Status code: 200

Table 4-83 Response body parameters

Parameter	Type	Description
login_profile	**LoginProfile** object	IAM user login information.

Table 4-84 LoginProfile

Parameter	Type	Description
user_id	String	IAM user ID.
password_reset_required	Boolean	Indicates whether an IAM user needs to change their password upon the next login.
password_expires_at	String	Time when the password of an IAM user expires.
created_at	String	Time when the IAM user login information was created.

Status code: 400

Table 4-85 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-86 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-87 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Modifying the login information of a specified IAM user. The password is set to **Password0** and the user is asked to change the password upon the next login.

```
PUT https://{endpoint}/v5/users/{user_id}/login-profile

{
  "password" : "Password0",
  "password_reset_required" : true
}
```

Example Responses

Status code: 200

Successful

```
{
  "login_profile" : {
    "user_id" : "user",
    "password_reset_required" : true,
    "password_expires_at" : "2023-09-13T08:03:10.781Z",
    "created_at" : "2023-09-13T08:03:10.781Z"
  }
}
```


Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.2.10 Deleting the Login Information of an IAM User

Function

This API is used to delete the login information of a specified IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:deleteLoginProfileV5	Write	user *	g:ResourceTag/<tag-key>	-	-

URI

DELETE /v5/users/{user_id}/login-profile

Table 4-88 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Request Parameters

None

Response Parameters

Status code: 204

Successful

Status code: 403

Table 4-89 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-90 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Deleting the login information of a specified IAM user

```
DELETE https://{endpoint}/v5/users/{user_id}/login-profile
```

Example Responses

None

Status Codes

Status Code	Description
204	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.3 Managing MFA Devices

4.1.3.1 Listing All Virtual MFA Devices

Function

This API is used to list all virtual MFA devices.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:mfa:listMFADevicesV5	List	mfa *	-	-	-

URI

GET /v5/mfa-devices

Table 4-91 Query Parameters

Parameter	Mandatory	Type	Description
user_id	No	String	IAM user ID.

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The value ranges from 1 to 200. The default value is 100. Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Pagination marker. The value contains 4 to 400 characters, including only letters, digits, and the following special characters: +/=-_ Minimum: **4** Maximum: **400**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-92 Response body parameters

Parameter	Type	Description
mfa_devices	Array of **MfaDeviceMetadata** objects	List of virtual MFA devices.
page_info	**PageInfo** object	Pagination information.

Table 4-93 MfaDeviceMetadata

Parameter	Type	Description
serial_number	String	Serial number of a virtual MFA device.
user_id	String	IAM user ID.
enabled	Boolean	Indicates whether a virtual MFA device is enabled.

Table 4-94 PageInfo

Parameter	Type	Description
next_marker	String	If this parameter exists, there are subsequent items that are not displayed in the current response body. The value can be used as the pagination marker parameter for the next request to obtain information about the next page. This API can be repeatedly called until this field does not exist.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-95 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-96 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Example Requests

- Listing all virtual MFA devices

  ```
  GET https://{endpoint}/v5/mfa-devices
  ```

- Listing all virtual MFA devices of IAM user *xxx*

  ```
  GET https://{endpoint}/v5/mfa-devices?user_id=xxx
  ```


Example Responses

Status code: 200

Successful

```
{
  "mfa_devices" : [ {
    "serial_number" : "iam::accountid:mfa:name",
    "user_id" : "xxx",
    "enabled" : true
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden

Error Codes

See **Error Codes**.

4.1.3.2 Enabling a Virtual MFA Device

Function

This API is used to enable a specified virtual MFA device and associate it with a specified IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:mfa:enableV5	Write	mfa *	-	-	-

URI

POST /v5/mfa-devices/enable

Request Parameters

Table 4-97 Request body parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.
serial_number	Yes	String	Serial number of a virtual MFA device. Maximum: **150**
authentication_code_first	Yes	String	Verification code sent by a device. Maximum: **12**
authentication_code_second	Yes	String	Subsequent verification code sent by a device. Maximum: **12**

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-98 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-99 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-100 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Enabling the virtual MFA device whose serial number is **iam::accountid:mfa:name** and associating it with IAM user *xxx*

```
POST https://{endpoint}/v5/mfa-devices/enable

{
  "user_id" : "xxx",
  "serial_number" : "iam::accountid:mfa:name",
  "authentication_code_first" : "123456",
  "authentication_code_second" : "123456"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.3.3 Disabling a Virtual MFA Device

Function

This API is used to disable a specified virtual MFA device and disassociate it from the corresponding IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:mfa:disableV5	Write	mfa *	-	-	-

URI

POST /v5/mfa-devices/disable

Request Parameters

Table 4-101 Request body parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.
serial_number	Yes	String	Serial number of a virtual MFA device. Maximum: **150**

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-102 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 403

Table 4-103 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-104 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Disabling the virtual MFA device whose serial number is **iam::accountid:mfa:name** and disassociating it from IAM user *xxx*

```
POST https://{endpoint}/v5/mfa-devices/disable

{
  "user_id" : "xxx",
  "serial_number" : "iam::accountid:mfa:name"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.3.4 Creating a Virtual MFA Device

Function

This API is used to create a virtual MFA device.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:mfa:createVirtualMFADeviceV5	Write	mfa *	-	-	-

URI

POST /v5/virtual-mfa-devices

Request Parameters

Table 4-105 Request body parameters

Parameter	Mandatory	Type	Description
virtual_mfa_device_name	Yes	String	Virtual MFA device name. The value contains 1 to 64 characters, including only letters, digits, underscores (_), and hyphens (-). Minimum: **1** Maximum: **64**
user_id	Yes	String	IAM user ID.

Response Parameters

Status code: 201

Table 4-106 Response body parameters

Parameter	Type	Description
virtual_mfa_device	**VirtualMfaDevice** object	Virtual MFA device.

Table 4-107 VirtualMfaDevice

Parameter	Type	Description
serial_number	String	Serial number of a virtual MFA device.
base32_string_seed	String	Key information, which a third-party system can use to generate an image verification code.

Status code: 400

Table 4-108 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-109 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-110 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-111 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Creating a virtual MFA device **name** for IAM user *xxx*

```
POST https://{endpoint}/v5/virtual-mfa-devices

{
  "virtual_mfa_device_name" : "name",
  "user_id" : "xxx"
}
```


Example Responses

Status code: 201

Successful

```
{
  "virtual_mfa_device" : {
    "serial_number" : "iam::accountid:mfa:name",
    "base32_string_seed" : "seed"
  }
}
```

Status Codes

Status Code	Description
201	Successful
400	Bad request
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.3.5 Deleting a Virtual MFA Device

Function

This API is used to delete a virtual MFA device.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:mfa:deleteVirtualMFADeviceV5	Write	mfa *	-	-	-

URI

DELETE /v5/virtual-mfa-devices

Table 4-112 Query Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.
serial_number	Yes	String	Serial number of a virtual MFA device. Maximum: **150**

Request Parameters

None

Response Parameters

Status code: 204

Successful

Status code: 400

Table 4-113 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-114 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-115 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Deleting the virtual MFA device whose serial number is **iam::accountid:mfa:name** for IAM user *xxx*

```
DELETE https://{endpoint}/v5/virtual-mfa-devices?user_id=xxx&serial_number=iam%3A%3Aaccountid%3Amfa%3Aname
```

Example Responses

None

Status Codes

Status Code	Description
204	Successful
400	Bad request
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.4 Changing Security Settings

4.1.4.1 Querying the Account Password Policy

Function

This API is used to query the account password policy.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:securitypolicies:getPasswordPolicyV5	Read	-	-	-	-

URI

GET /v5/password-policy

Request Parameters

None

Response Parameters

Status code: 200

Table 4-116 Response body parameters

Parameter	Type	Description
password_policy	**PasswordPolicy** object	Password policy.

Table 4-117 PasswordPolicy

Parameter	Type	Description
maximum_consecutive_identical_chars	Integer	Maximum number of consecutive identical characters.
maximum_password_length	Integer	Maximum number of characters that a password can contain.
minimum_password_age	Integer	Minimum password age (minute).
minimum_password_length	Integer	Minimum number of characters that a password must contain.

Parameter	Type	Description
password_reuse_prevention	Integer	Number of recent passwords disallowed.
password_not_username_or_invert	Boolean	Whether to disallow the username or the username spelled backwards for passwords. The default value is **true**, indicating that the password cannot be the username or the username spelled backwards.
password_requirements	String	Characters that a password must contain.
password_validity_period	Integer	Password validity period (days).
password_char_combination	Integer	Minimum number of character types that a password must contain.
allow_user_to_change_password	Boolean	Indicates whether IAM users are allowed to change their passwords. This is not applicable to the root user.

Status code: 403

Table 4-118 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Example Requests

Querying the account password policy

```
GET https://{endpoint}/v5/password-policy
```

Example Responses

Status code: 200

Successful


```
{
  "password_policy" : {
    "maximum_consecutive_identical_chars" : 0,
    "maximum_password_length" : 32,
    "minimum_password_age" : 0,
    "minimum_password_length" : 8,
    "password_reuse_prevention" : 1,
    "password_not_username_or_invert" : true,
    "password_requirements" : "A password must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters.",
    "password_validity_period" : 180,
    "password_char_combination" : 2,
    "allow_user_to_change_password" : true
  }
}
```

Status Codes

Status Code	Description
200	Successful
403	Forbidden

Error Codes

See **Error Codes**.

4.1.4.2 Modifying the Account Password Policy

Function

This API is used to modify the account password policy.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:securitypolicies:updatePasswordPolicyV5	Write	-	-	-	-

URI

PUT /v5/password-policy

Request Parameters

Table 4-119 Request body parameters

Parameter	Mandatory	Type	Description
maximum_consecutive_identical_chars	No	Integer	The maximum number of times that a character is allowed to consecutively present in a password. Value range: [0,32]. Minimum: **0** Maximum: **32**
minimum_password_age	No	Integer	The minimum period (minutes) after which users are allowed to make a password change. Value range: [0,1440]. Minimum: **0** Maximum: **1440**
minimum_password_length	No	Integer	The minimum number of characters that a password must contain. Value range: [8,32]. Minimum: **8** Maximum: **32**
password_reuse_prevention	No	Integer	The number of times that a password cannot be reused. Value range: [0,24]. Minimum: **0** Maximum: **24**
password_not_username_or_invert	No	Boolean	Whether to disallow the username or the username spelled backwards for passwords. The default value is **true**, indicating that the password cannot be the username or the username spelled backwards.
password_validity_period	No	Integer	Password validity period (days). Value range: [0,180]. Minimum: **0** Maximum: **180**

Parameter	Mandatory	Type	Description
password_char_combination	No	Integer	The minimum number of character types that a password must contain. Value range: [2,4]. Minimum: **2** Maximum: **4**
allow_user_to_change_password	No	Boolean	Indicates whether IAM users are allowed to change their passwords. This is not applicable to the root user.

Response Parameters

Status code: 200

Table 4-120 Response body parameters

Parameter	Type	Description
password_policy	**PasswordPolicy** object	Password policy.

Table 4-121 PasswordPolicy

Parameter	Type	Description
maximum_consecutive_identical_chars	Integer	Maximum number of consecutive identical characters.
maximum_password_length	Integer	Maximum number of characters that a password can contain.
minimum_password_age	Integer	Minimum password age (minute).
minimum_password_length	Integer	Minimum number of characters that a password must contain.
password_reuse_prevention	Integer	Number of recent passwords disallowed.

Parameter	Type	Description
password_not_username_or_invert	Boolean	Whether to disallow the username or the username spelled backwards for passwords. The default value is **true**, indicating that the password cannot be the username or the username spelled backwards.
password_requirements	String	Characters that a password must contain.
password_validity_period	Integer	Password validity period (days).
password_char_combination	Integer	Minimum number of character types that a password must contain.
allow_user_to_change_password	Boolean	Indicates whether IAM users are allowed to change their passwords. This is not applicable to the root user.

Status code: 400

Table 4-122 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-123 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Example Requests

Modifying the account password policy

```
PUT https://{endpoint}/v5/password-policy

{
  "maximum_consecutive_identical_chars" : 0,
  "minimum_password_age" : 0,
  "minimum_password_length" : 8,
  "password_reuse_prevention" : 1,
  "password_not_username_or_invert" : true,
  "password_validity_period" : 180,
  "password_char_combination" : 2,
  "allow_user_to_change_password" : true
}
```

Example Responses

Status code: 200

Successful

```
{
  "password_policy" : {
    "maximum_consecutive_identical_chars" : 0,
    "maximum_password_length" : 32,
    "minimum_password_age" : 0,
    "minimum_password_length" : 8,
    "password_reuse_prevention" : 1,
    "password_not_username_or_invert" : true,
    "password_requirements" : "A password must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters.",
    "password_validity_period" : 180,
    "password_char_combination" : 2,
    "allow_user_to_change_password" : true
  }
}
```

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden

Error Codes

See **Error Codes**.

4.1.4.3 Querying the Account Login Policy

Function

This API is used to query the account login policy.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:securitypolicies:getLoginPolicyV5	Read	-	-	-	-

URI

GET /v5/login-policy

Request Parameters

None

Response Parameters

Status code: 200

Table 4-124 Response body parameters

Parameter	Type	Description
login_policy	**LoginPolicy** object	Login authentication policy

Table 4-125 LoginPolicy

Parameter	Type	Description
user_validity_period	Integer	If an IAM user does not log in within the validity period (days) specified by this parameter, the user is disabled. This does not apply to the root user.
custom_info_for_login	String	Login information.
lockout_duration	Integer	Account lockout duration (minute) for IAM users.

Parameter	Type	Description
login_failed_times	Integer	Maximum number of invalid login attempts.
period_with_login_failures	Integer	Specified duration (minute).
session_timeout	Integer	Timeout duration of a session.
show_recent_login_info	Boolean	Indicates whether to display the last login information upon successful login.
allow_address_netmasks	Array of **AllowAddressNetmask** objects	IP addresses or CIDR blocks from which API access is allowed.
allow_ip_ranges	Array of **AllowIpRange** objects	IP address ranges from which API access is allowed.

Table 4-126 AllowAddressNetmask

Parameter	Type	Description
address_netmask	String	IP address or CIDR block, for example, **192.168.0.1/24**. Maximum: **50**
description	String	Description. The value cannot contain the following special characters: @# %&<>\$^* Maximum: **255**

Table 4-127 AllowIpRange

Parameter	Type	Description
ip_range	String	IP address range, for example, **0.0.0.0-255.255.255.255** Maximum: **50**
description	String	Description. The value cannot contain the following special characters: @# %&<>\$^* Maximum: **255**

Status code: 403

Table 4-128 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Example Requests

Querying the account login policy

```
GET https://{endpoint}/v5/login-policy
```

Example Responses

Status code: 200

Successful

```
{
  "login_policy" : {
    "user_validity_period" : 0,
    "custom_info_for_login" : "info",
    "lockout_duration" : 15,
    "login_failed_times" : 5,
    "period_with_login_failures" : 15,
    "session_timeout" : 60,
    "show_recent_login_info" : false,
    "allow_address_netmasks" : [ {
      "address_netmask" : "192.168.0.1/24",
      "description" : "description"
    } ],
    "allow_ip_ranges" : [ {
      "ip_range" : "0.0.0.0-255.255.255.255",
      "description" : "description"
    } ]
  }
}
```

Status Codes

Status Code	Description
200	Successful
403	Forbidden

Error Codes

See **Error Codes**.

4.1.4.4 Modifying the Account Login Policy

Function

This API is used to modify the account login policy.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:securitypolicies:updateLoginPolicyV5	Write	-	-	-	-

URI

PUT /v5/login-policy

Request Parameters

Table 4-129 Request body parameters

Parameter	Mandatory	Type	Description
user_validity_period	No	Integer	If an IAM user does not log in within the specified validity period (days), the user is disabled. Value range: [0,240]. This parameter does not apply to the root user. Minimum: **0** Maximum: **240**
custom_info_for_login	No	String	Login information. The value cannot contain the following special characters: @#%&<>\$^* Maximum: **64**

Parameter	Mandatory	Type	Description
lockout_duration	No	Integer	IAM user login lockout duration (minutes). The value range is [15,1440]. Minimum: **15** Maximum: **1440**
login_failed_times	No	Integer	Number of unsuccessful login attempts to lock users out. Value range: [3,10]. Minimum: **3** Maximum: **10**
period_with_login_failures	No	Integer	Period (minutes) to count the number of unsuccessful login attempts. Value range: [15,60]. Minimum: **15** Maximum: **60**
session_timeout	No	Integer	Session timeout (minutes) that will apply if you or users created using your account do not perform any operations within a specific period. Value range: [15,1440]. Minimum: **15** Maximum: **1440**
show_recent_login_info	No	Boolean	Indicates whether to display the last login information upon successful login.
allow_address_netmasks	No	Array of **AllowAddressNetmask** objects	IP address or CIDR block that is allowed to access, for example, xxx.xxx.xxx.xxx/24.
allow_ip_ranges	No	Array of **AllowIpRange** objects	IP address range that is allowed to access, for example, 0.0.0.0-255.255.255.255.

Table 4-130 AllowAddressNetmask

Parameter	Mandatory	Type	Description
address_netmask	Yes	String	IP address or CIDR block, for example, **192.168.0.1/24**. Maximum: **50**
description	No	String	Description. The value cannot contain the following special characters: @#%&<>\$^* Maximum: **255**

Table 4-131 AllowIpRange

Parameter	Mandatory	Type	Description
ip_range	Yes	String	IP address range, for example, **0.0.0.0-255.255.255.255** Maximum: **50**
description	No	String	Description. The value cannot contain the following special characters: @#%&<>\$^* Maximum: **255**

Response Parameters

Status code: 200

Table 4-132 Response body parameters

Parameter	Type	Description
login_policy	**LoginPolicy** object	Login authentication policy

Table 4-133 LoginPolicy

Parameter	Type	Description
user_validity_period	Integer	If an IAM user does not log in within the validity period (days) specified by this parameter, the user is disabled. This does not apply to the root user.
custom_info_for_login	String	Login information.

Parameter	Type	Description
lockout_duration	Integer	Account lockout duration (minute) for IAM users.
login_failed_times	Integer	Maximum number of invalid login attempts.
period_with_login_failures	Integer	Specified duration (minute).
session_timeout	Integer	Timeout duration of a session.
show_recent_login_info	Boolean	Indicates whether to display the last login information upon successful login.
allow_address_netmasks	Array of **AllowAddressNetmask** objects	IP addresses or CIDR blocks from which API access is allowed.
allow_ip_ranges	Array of **AllowIpRange** objects	IP address ranges from which API access is allowed.

Table 4-134 AllowAddressNetmask

Parameter	Type	Description
address_netmask	String	IP address or CIDR block, for example, **192.168.0.1/24**. Maximum: **50**
description	String	Description. The value cannot contain the following special characters: @# %&<>\$^* Maximum: **255**

Table 4-135 AllowIpRange

Parameter	Type	Description
ip_range	String	IP address range, for example, **0.0.0.0-255.255.255.255** Maximum: **50**
description	String	Description. The value cannot contain the following special characters: @# %&<>\$^* Maximum: **255**

Status code: 400

Table 4-136 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-137 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Example Requests

Modifying the account login policy

```
PUT https://{endpoint}/v5/login-policy

{
  "user_validity_period" : 0,
  "custom_info_for_login" : "info",
  "lockout_duration" : 15,
  "login_failed_times" : 5,
  "period_with_login_failures" : 15,
  "session_timeout" : 60,
  "show_recent_login_info" : false,
  "allow_address_netmasks" : [ {
    "address_netmask" : "192.168.0.1/24",
    "description" : "description"
  } ],
  "allow_ip_ranges" : [ {
    "ip_range" : "0.0.0.0-255.255.255.255",
    "description" : "description"
  } ]
}
```

Example Responses

Status code: 200

Successful

```
{
  "login_policy" : {
```



```
  "user_validity_period" : 0,
  "custom_info_for_login" : "info",
  "lockout_duration" : 15,
  "login_failed_times" : 5,
  "period_with_login_failures" : 15,
  "session_timeout" : 60,
  "show_recent_login_info" : false,
  "allow_address_netmasks" : [ {
    "address_netmask" : "192.168.0.1/24",
    "description" : "description"
  } ],
  "allow_ip_ranges" : [ {
    "ip_range" : "0.0.0.0-255.255.255.255",
    "description" : "description"
  } ]
 }
}
```

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden

Error Codes

See **Error Codes**.

4.1.5 Managing User Groups

4.1.5.1 Listing Groups

Function

This API is used to list groups.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:groups:listGroupsV5	List	group *	-	-	-

URI

GET /v5/groups

Table 4-138 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The value ranges from 1 to 200. The default value is 100. Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Pagination marker. The value contains 4 to 400 characters, including only letters, digits, and the following special characters: +/=-_ Minimum: **4** Maximum: **400**
user_id	No	String	IAM user ID.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-139 Response body parameters

Parameter	Type	Description
groups	Array of **Group** objects	Group list.
page_info	**PageInfo** object	Pagination information.

Table 4-140 Group

Parameter	Type	Description
group_id	String	Group ID.

Parameter	Type	Description
group_name	String	User group name. The value can contain 1 to 128 characters, including letters, digits, spaces, underscores (_), hyphens (-), and braces ({ and }).
created_at	String	Time when a group was created.
urn	String	Uniform resource name.
description	String	User group description. The value can contain 0 to 255 characters and cannot contain the following special characters: @, #, %, &, <, >, \, $, ^, and *.

Table 4-141 PageInfo

Parameter	Type	Description
next_marker	String	If this parameter exists, there are subsequent items that are not displayed in the current response body. The value can be used as the pagination marker parameter for the next request to obtain information about the next page. This API can be repeatedly called until this field does not exist.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-142 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-143 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Example Requests

- Listing all groups

  ```
  GET https://{endpoint}/v5/groups
  ```

- Listing all groups to which IAM user *xxx* belongs

  ```
  GET https://{endpoint}/v5/groups?user_id=xxx
  ```

Example Responses

Status code: 200

Successful

```
{
  "groups" : [ {
    "group_id" : "string",
    "group_name" : "name",
    "created_at" : "2023-09-11T10:13:25.414Z",
    "urn" : "iam::accountid:group:name",
    "description" : "description"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden

Error Codes

See **Error Codes**.

4.1.5.2 Creating a Group

Function

This API is used to create a group.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:groups:createGroupV5	Write	group *	-	-	-

URI

POST /v5/groups

Request Parameters

Table 4-144 Request body parameters

Parameter	Mandatory	Type	Description
group_name	Yes	String	User group name. The value can contain 1 to 128 characters, including letters, digits, spaces, underscores (_), hyphens (-), and braces ({ and }).
description	No	String	User group description. The value can contain 0 to 255 characters and cannot contain the following special characters: @, #, %, &, <, >, \, $, ^, and *.

Response Parameters

Status code: 201

Table 4-145 Response body parameters

Parameter	Type	Description
group	**Group** object	Group.

Table 4-146 Group

Parameter	Type	Description
group_id	String	Group ID.
group_name	String	User group name. The value can contain 1 to 128 characters, including letters, digits, spaces, underscores (_), hyphens (-), and braces ({ and }).
created_at	String	Time when a group was created.
urn	String	Uniform resource name.
description	String	User group description. The value can contain 0 to 255 characters and cannot contain the following special characters: @, #, %, &, <, >, \, $, ^, and *.

Status code: 400

Table 4-147 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-148 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 409

Table 4-149 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Creating a group **name**

```
POST https://{endpoint}/v5/groups

{
  "group_name" : "name",
  "description" : "description"
}
```

Example Responses

Status code: 201

Successful

```
{
  "group" : {
    "group_id" : "string",
    "group_name" : "name",
    "created_at" : "2023-09-11T10:13:25.414Z",
    "urn" : "iam::accountid:group:name",
    "description" : "description"
  }
}
```

Status Codes

Status Code	Description
201	Successful
400	Bad request

Status Code	Description
403	Forbidden
409	Conflict

Error Codes

See **Error Codes**.

4.1.5.3 Querying Group Details

Function

This API is used to query group details.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:groups:getGroupV5	Read	group *	-	-	-

URI

GET /v5/groups/{group_id}

Table 4-150 Path Parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	Group ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

None

Response Parameters

Status code: 200

Table 4-151 Response body parameters

Parameter	Type	Description
group	**Group** object	Group.

Table 4-152 Group

Parameter	Type	Description
group_id	String	Group ID.
group_name	String	User group name. The value can contain 1 to 128 characters, including letters, digits, spaces, underscores (_), hyphens (-), and braces ({ and }).
created_at	String	Time when a group was created.
urn	String	Uniform resource name.
description	String	User group description. The value can contain 0 to 255 characters and cannot contain the following special characters: @, #, %, &, <, >, \, $, ^, and *.

Status code: 403

Table 4-153 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-154 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying group details

```
GET https://{endpoint}/v5/groups/{group_id}
```

Example Responses

Status code: 200

Successful

```
{
  "group" : {
    "group_id" : "string",
    "group_name" : "name",
    "created_at" : "2023-09-11T10:13:25.414Z",
    "urn" : "iam::accountid:group:name",
    "description" : "description"
  }
}
```

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.5.4 Modifying a Group

Function

This API is used to modify a group.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:groups:updateGroupV5	Write	group *	-	-	-

URI

PUT /v5/groups/{group_id}

Table 4-155 Path Parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	Group ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

Table 4-156 Request body parameters

Parameter	Mandatory	Type	Description
new_group_name	No	String	User group name. The value can contain 1 to 128 characters, including letters, digits, spaces, underscores (_), hyphens (-), and braces ({ and }).
new_group_description	No	String	User group description. The value can contain 0 to 255 characters and cannot contain the following special characters: @, #, %, &, <, >, \, $, ^, and *.

Response Parameters

Status code: 200

Table 4-157 Response body parameters

Parameter	Type	Description
group	**Group** object	Group.

Table 4-158 Group

Parameter	Type	Description
group_id	String	Group ID.
group_name	String	User group name. The value can contain 1 to 128 characters, including letters, digits, spaces, underscores (_), hyphens (-), and braces ({ and }).
created_at	String	Time when a group was created.
urn	String	Uniform resource name.
description	String	User group description. The value can contain 0 to 255 characters and cannot contain the following special characters: @, #, %, &, <, >, \, $, ^, and *.

Status code: 400

Table 4-159 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-160 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-161 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-162 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Modifying a group

```
PUT https://{endpoint}/v5/groups/{group_id}

{
  "new_group_name" : "name",
  "new_group_description" : "description"
}
```

Example Responses

Status code: 200

Successful

```
{
  "group" : {
```

```
  "group_id" : "string",
  "group_name" : "name",
  "created_at" : "2023-09-11T10:13:25.414Z",
  "urn" : "iam::accountid:group:name",
  "description" : "description"
 }
}
```

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.5.5 Deleting a Group

Function

This API is used to delete a group.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:groups:deleteGroupV5	Write	group *	-	-	-

URI

DELETE /v5/groups/{group_id}

Table 4-163 Path Parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	Group ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

None

Response Parameters

Status code: 204

Successful

Status code: 403

Table 4-164 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-165 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-166 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Deleting a group

```
DELETE https://{endpoint}/v5/groups/{group_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.5.6 Adding an IAM User to a Group

Function

This API is used to add an IAM user to a group.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:permissions:addUserToGroupV5	Write	group *	-	-	-

URI

POST /v5/groups/{group_id}/add-user

Table 4-167 Path Parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	Group ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

Table 4-168 Request body parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-169 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-170 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-171 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-172 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Adding IAM user *xxx* to a specified group

```
POST https://{endpoint}/v5/groups/{group_id}/add-user

{
  "user_id" : "xxx"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found
409	Request conflicts occurred.

Error Codes

See **Error Codes**.

4.1.5.7 Removing an IAM User from a Group

Function

This API is used to remove an IAM user from a group.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:permissions:removeUserFromGroupV5	Write	group *	-	-	-

URI

POST /v5/groups/{group_id}/remove-user

Table 4-173 Path Parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	Group ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

Table 4-174 Request body parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Response Parameters

Status code: 200

Successful

Status code: 403

Table 4-175 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-176 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Removing IAM user *xxx* from a specified group

```
POST https://{endpoint}/v5/groups/{group_id}/remove-user

{
  "user_id" : "xxx"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.6 Managing Identity Policies

4.1.6.1 Querying All Identity Policies

Function

This API is used to query all identity policies, including system-defined identity policies and custom identity policies.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:policies:listV5	List	policy *	-	-	-

URI

GET /v5/policies

Table 4-177 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The value ranges from 1 to 200. The default value is 100. Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Pagination marker. The value contains 4 to 400 characters, including only letters, digits, and the following special characters: +/=-_ Minimum: **4** Maximum: **400**
policy_type	No	String	Identity policy type. The value can be custom or system-defined.
path_prefix	No	String	Resource path prefix, which consists of multiple character strings. Each character string must end with a slash (/) and can only contain letters, digits, and the following special characters: .,+@=_-, for example, **foo/bar/**. Maximum: **512**
only_attached	No	Boolean	Indicates whether to only list the identity policies with entities attached. Default: **false**

Request Parameters

Table 4-178 Request header parameters

Parameter	Mandatory	Type	Description
X-Language	No	String	Language of the returned message. The value can be **zh-cn** or **en-us** and is **zh-cn** by default. Default: **zh-cn**

Response Parameters

Status code: 200

Table 4-179 Response body parameters

Parameter	Type	Description
policies	Array of **Policy** objects	Identity policy list.
page_info	**PageInfo** object	Pagination information.

Table 4-180 Policy

Parameter	Type	Description
policy_type	String	Identity policy type. The value can be custom or system-defined.
policy_name	String	Identity policy name. The value contains 1 to 128 characters, including only letters, digits, and the following special characters: _+=.@-
policy_id	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
urn	String	Uniform resource name.
path	String	Resource path, which is an empty string by default. It consists of multiple character strings. Each character string must end with a slash (/) and can only contain letters, digits, and the following special characters: .,+@=_-, for example, **foo/bar/**.

Parameter	Type	Description
default_version_id	String	Default version number.
attachment_count	Integer	Number of entities to which an identity policy is attached.
description	String	Identity policy description.
created_at	String	Time when an identity policy was created.
updated_at	String	Time when the default version of an identity policy was last updated.

Table 4-181 PageInfo

Parameter	Type	Description
next_marker	String	If this parameter exists, there are subsequent items that are not displayed in the current response body. The value can be used as the pagination marker parameter for the next request to obtain information about the next page. This API can be repeatedly called until this field does not exist.
current_count	Integer	Number of items returned on this page.

Status code: 403

Table 4-182 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Example Requests

Querying all identity policies


```
GET https://{endpoint}/v5/policies
```

Example Responses

Status code: 200

Successful

```
{
  "policies" : [ {
    "policy_type" : "custom",
    "policy_name" : "name",
    "policy_id" : "string",
    "urn" : "iam::accountid:policy:name",
    "path" : "",
    "default_version_id" : "v1",
    "attachment_count" : 0,
    "description" : "description",
    "created_at" : "2023-09-25T07:49:11.582Z",
    "updated_at" : "2023-09-25T07:49:11.582Z"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful
403	Forbidden

Error Codes

See **Error Codes**.

4.1.6.2 Creating a Custom Identity Policy

Function

This API is used to create a custom identity policy whose default version is **v1**.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:policies:createV5	Permission_management	policy *	-	-	-

URI

POST /v5/policies

Request Parameters

Table 4-183 Request body parameters

Parameter	Mandatory	Type	Description
policy_name	Yes	String	Identity policy name. The value contains 1 to 128 characters, including only letters, digits, and the following special characters: _ +=.@-
path	No	String	Resource path, which is an empty string by default. It consists of multiple character strings. Each character string must end with a slash (/) and can only contain letters, digits, and the following special characters: .,+@=_-, for example, **foo/bar/**.

Parameter	Mandatory	Type	Description

policy_document	Yes	String	JSON format of the policy document of a custom or a preset identity policy. Characters =, <, >, (,), and | are special characters in the grammar and are not included in policies.
			The question mark (?) following an element indicates that the element is optional, for example, **sid_block?**.
			The vertical bar (|) separates options, and the parentheses enclose the options, for example, **("Allow" | "Deny")**.
			When an element allows more than one value, use commas (,), and ellipsis (...), for example, **[<policy_statement>, <policy_statement>, ...]**.
			The following listing describes the policy language grammar:
			policy = {
			  <version_block>,
			  <statement_block>
			}
			
			<version_block> = "Version" : ("5.0")
			
			<statement_block> = "Statement" :
			[<policy_statement>,
			<policy_statement>, ...]
			
			<policy_statement> = {
			  <sid_block?>,
			  <effect_block>,
			  <action_block>,
			  <resource_block?>,
			  <condition_block?>
			}
			
			<sid_block> = "Sid" : <sid_string>
			
			<effect_block> = "Effect" : ("Allow" |
			"Deny")
			
			<action_block> = ("Action" |
			"NotAction") : [<action_string>,
			<action_string>, ...]
			
			<resource_block> = ("Resource" |
			"NotResource") : [<resource_string>,
			<resource_string>, ...]
			
			<condition_block> = "Condition" :
			{ <condition_map> }

Parameter	Mandatory	Type	Description

			<condition_map> = {
			  <condition_type_string> :
			{ <condition_key_string> :
			<condition_value_list> },
			  <condition_type_string> :
			{ <condition_key_string> :
			<condition_value_list> },
			  ...
			}
			
			<condition_value_list> =
			(<condition_value> |
			[<condition_value>,
			<condition_value>, ...])
			
			<condition_value> = "string"

description	No	String	Identity policy description.

Response Parameters

Status code: 201

Table 4-184 Response body parameters

Parameter	Type	Description
policy	**Policy** object	Identity policy.

Table 4-185 Policy

Parameter	Type	Description
policy_type	String	Identity policy type. The value can be custom or system-defined.
policy_name	String	Identity policy name. The value contains 1 to 128 characters, including only letters, digits, and the following special characters: _+=.@-
policy_id	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
urn	String	Uniform resource name.

Parameter	Type	Description
path	String	Resource path, which is an empty string by default. It consists of multiple character strings. Each character string must end with a slash (/) and can only contain letters, digits, and the following special characters: .,+@=_-, for example, **foo/bar/**.
default_version_id	String	Default version number.
attachment_count	Integer	Number of entities to which an identity policy is attached.
description	String	Identity policy description.
created_at	String	Time when an identity policy was created.
updated_at	String	Time when the default version of an identity policy was last updated.

Status code: 400

Table 4-186 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-187 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 409

Table 4-188 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Creating a custom identity policy **name**

```
POST https://{endpoint}/v5/policies

{
  "policy_name" : "name",
  "path" : "",
  "policy_document" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"*\"]}]}",
  "description" : "description"
}
```

Example Responses

Status code: 201

Successful

```
{
  "policy" : {
    "policy_type" : "custom",
    "policy_name" : "name",
    "policy_id" : "string",
    "urn" : "iam::accountid:policy:name",
    "path" : "",
    "default_version_id" : "v1",
    "attachment_count" : 0,
    "description" : "description",
    "created_at" : "2023-09-25T07:49:11.582Z",
    "updated_at" : "2023-09-25T07:49:11.582Z"
  }
}
```

Status Codes

Status Code	Description
201	Successful
400	Bad request
403	Forbidden
409	Conflict

Error Codes

See **Error Codes**.

4.1.6.3 Obtaining an Identity Policy Based on the Identity Policy ID

Function

This API is used to obtain an identity policy based on the identity policy ID.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:policies:getV5	Read	policy *	-	-	-

URI

GET /v5/policies/{policy_id}

Table 4-189 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

Table 4-190 Request header parameters

Parameter	Mandatory	Type	Description
X-Language	No	String	Language of the returned message. The value can be **zh-cn** or **en-us** and is **zh-cn** by default. Default: **zh-cn**

Response Parameters

Status code: 200

Table 4-191 Response body parameters

Parameter	Type	Description
policy	**Policy** object	Identity policy.

Table 4-192 Policy

Parameter	Type	Description
policy_type	String	Identity policy type. The value can be custom or system-defined.
policy_name	String	Identity policy name. The value contains 1 to 128 characters, including only letters, digits, and the following special characters: _+=.@-
policy_id	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
urn	String	Uniform resource name.
path	String	Resource path, which is an empty string by default. It consists of multiple character strings. Each character string must end with a slash (/) and can only contain letters, digits, and the following special characters: .,+@=_-, for example, **foo/bar/**.
default_version_id	String	Default version number.
attachment_count	Integer	Number of entities to which an identity policy is attached.
description	String	Identity policy description.
created_at	String	Time when an identity policy was created.
updated_at	String	Time when the default version of an identity policy was last updated.

Status code: 403

Table 4-193 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-194 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Obtaining an identity policy based on the identity policy ID

```
GET https://{endpoint}/v5/policies/{policy_id}
```

Example Responses

Status code: 200

Successful

```
{
  "policy" : {
    "policy_type" : "custom",
    "policy_name" : "name",
    "policy_id" : "string",
    "urn" : "iam::accountid:policy:name",
    "path" : "",
    "default_version_id" : "v1",
    "attachment_count" : 0,
    "description" : "description",
    "created_at" : "2023-09-25T07:49:11.582Z",
    "updated_at" : "2023-09-25T07:49:11.582Z"
  }
}
```


Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.6.4 Deleting a Custom Identity Policy

Function

This API is used to delete a custom identity policy. Ensure that it is not attached to any IAM users, groups, agencies, or trust agencies.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:policies:deleteV5	Permission_management	policy *	-	-	-

URI

DELETE /v5/policies/{policy_id}

Table 4-195 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

None

Response Parameters

Status code: 204

Successful

Status code: 403

Table 4-196 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-197 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-198 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Deleting a specified custom identity policy

```
DELETE https://{endpoint}/v5/policies/{policy_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.6.5 Creating a Version for a Specified Identity Policy

Function

This API is used to create a version for a specified identity policy.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:policies:createVersionV5	Permission_management	policy *	-	-	-

URI

POST /v5/policies/{policy_id}/versions

Table 4-199 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

Table 4-200 Request body parameters

Parameter	Mandatory	Type	Description

policy_document	Yes	String	JSON format of the policy document of a custom or a preset identity policy. Characters =, <, >, (,), and | are special characters in the grammar and are not included in policies.
			The question mark (?) following an element indicates that the element is optional, for example, **sid_block?**.
			The vertical bar (|) separates options, and the parentheses enclose the options, for example, **("Allow" | "Deny")**.
			When an element allows more than one value, use commas (,), and ellipsis (...), for example, **[<policy_statement>, <policy_statement>, ...]**.
			The following listing describes the policy language grammar:
			policy = {
			  <version_block>,
			  <statement_block>
			}
			
			<version_block> = "Version" : ("5.0")
			
			<statement_block> = "Statement" :
			[<policy_statement>,
			<policy_statement>, ...]
			
			<policy_statement> = {
			  <sid_block?>,
			  <effect_block>,
			  <action_block>,
			  <resource_block?>,
			  <condition_block?>
			}
			
			<sid_block> = "Sid" : <sid_string>
			
			<effect_block> = "Effect" : ("Allow" |
			"Deny")
			
			<action_block> = ("Action" |
			"NotAction") : [<action_string>,
			<action_string>, ...]
			
			<resource_block> = ("Resource" |
			"NotResource") : [<resource_string>,

Parameter	Mandatory	Type	Description

			<resource_string>, ...]
			
			<condition_block> = "Condition" :
			{ <condition_map> }
			
			<condition_map> = {
			  <condition_type_string> :
			{ <condition_key_string> :
			<condition_value_list> },
			  <condition_type_string> :
			{ <condition_key_string> :
			<condition_value_list> },
			  ...
			}
			
			<condition_value_list> =
			(<condition_value> |
			[<condition_value>,
			<condition_value>, ...])
			
			<condition_value> = "string"

set_as_default	No	Boolean	Indicates whether to set the version as the default version. Default: **false**

Response Parameters

Status code: 201

Table 4-201 Response body parameters

Parameter	Type	Description
policy_version	**PolicyVersion** object	Identity policy version.

Table 4-202 PolicyVersion

Parameter	Type	Description

document	String	JSON format of the policy document of a custom or a preset identity policy. Characters =, <, >, (,), and | are special characters in the grammar and are not included in policies.
		The question mark (?) following an element indicates that the element is optional, for example, **sid_block?**.
		The vertical bar (|) separates options, and the parentheses enclose the options, for example, **("Allow" | "Deny")**.
		When an element allows more than one value, use commas (,), and ellipsis (...), for example, **[<policy_statement>, <policy_statement>, ...]**.
		The following listing describes the policy language grammar:
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :
		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}

Parameter	Type	Description
		<condition_value_list> = (<condition_value> | [<condition_value>, <condition_value>, ...]) <condition_value> = "string"
version_id	String	Identity policy version. The value is a character string starting with **v** and followed by digits, for example, **v5**.
is_default	Boolean	Indicates whether the version is the default version.
created_at	String	Time when an identity policy version was created.

Status code: 400

Table 4-203 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-204 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-205 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-206 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Creating a version for a specified identity policy and setting it as the default version

```
POST https://{endpoint}/v5/policies/{policy_id}/versions

{
  "policy_document" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"*\"]}]}",
  "set_as_default" : true
}
```

Example Responses

Status code: 201

Successful

```
{
  "policy_version" : {
    "document" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"*\"]}]}",
    "version_id" : "v2",
    "is_default" : true,
    "created_at" : "2023-09-25T08:00:51.537Z"
  }
}
```

Status Codes

Status Code	Description
201	Successful

Status Code	Description
400	Bad request
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.6.6 Querying All Versions of a Specified Identity Policy

Function

This API is used to query all versions of a specified identity policy.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:policies:listVersionsV5	List	policy *	-	-	-

URI

GET /v5/policies/{policy_id}/versions

Table 4-207 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Table 4-208 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The value ranges from 1 to 200. The default value is 100. Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Pagination marker. The value contains 4 to 400 characters, including only letters, digits, and the following special characters: +/=-_ Minimum: **4** Maximum: **400**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-209 Response body parameters

Parameter	Type	Description
versions	Array of **PolicyVersion** objects	List of identity policy versions.
page_info	**PageInfo** object	Pagination information.

Table 4-210 PolicyVersion

Parameter	Type	Description

document	String	JSON format of the policy document of a custom or a preset identity policy. Characters =, <, >, (,), and | are special characters in the grammar and are not included in policies.
		The question mark (?) following an element indicates that the element is optional, for example, **sid_block?**.
		The vertical bar (|) separates options, and the parentheses enclose the options, for example, **("Allow" | "Deny")**.
		When an element allows more than one value, use commas (,), and ellipsis (...), for example, **[<policy_statement>, <policy_statement>, ...]**.
		The following listing describes the policy language grammar:
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :
		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}

Parameter	Type	Description
		<condition_value_list> = (<condition_value> | [<condition_value>, <condition_value>, ...]) <condition_value> = "string"
version_id	String	Identity policy version. The value is a character string starting with **v** and followed by digits, for example, **v5**.
is_default	Boolean	Indicates whether the version is the default version.
created_at	String	Time when an identity policy version was created.

Table 4-211 PageInfo

Parameter	Type	Description
next_marker	String	If this parameter exists, there are subsequent items that are not displayed in the current response body. The value can be used as the pagination marker parameter for the next request to obtain information about the next page. This API can be repeatedly called until this field does not exist.
current_count	Integer	Number of items returned on this page.

Status code: 403

Table 4-212 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-213 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying all versions of a specified identity policy

```
GET https://{endpoint}/v5/policies/{policy_id}/versions
```

Example Responses

Status code: 200

Successful

```
{
  "versions" : [ {
    "document" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"*\"]}]}",
    "version_id" : "v1",
    "is_default" : true,
    "created_at" : "2023-09-25T09:03:24.786Z"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.6.7 Querying the Version of a Specified Identity Policy

Function

This API is used to query the version information, including the identity policy document of a specified identity policy.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:policies:getVersionV5	Read	policy *	-	-	-

URI

GET /v5/policies/{policy_id}/versions/{version_id}

Table 4-214 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
version_id	Yes	String	Identity policy version. The value is a character string starting with **v** and followed by digits, for example, **v5**.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-215 Response body parameters

Parameter	Type	Description
policy_version	**PolicyVersion** object	Identity policy version.

Table 4-216 PolicyVersion

Parameter	Type	Description

document	String	JSON format of the policy document of a custom or a preset identity policy. Characters =, <, >, (,), and | are special characters in the grammar and are not included in policies.
		The question mark (?) following an element indicates that the element is optional, for example, **sid_block?**.
		The vertical bar (|) separates options, and the parentheses enclose the options, for example, **("Allow" | "Deny")**.
		When an element allows more than one value, use commas (,), and ellipsis (...), for example, **[<policy_statement>, <policy_statement>, ...]**.
		The following listing describes the policy language grammar:
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :
		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}

Parameter	Type	Description
		<condition_value_list> = (<condition_value> | [<condition_value>, <condition_value>, ...]) <condition_value> = "string"
version_id	String	Identity policy version. The value is a character string starting with **v** and followed by digits, for example, **v5**.
is_default	Boolean	Indicates whether the version is the default version.
created_at	String	Time when an identity policy version was created.

Status code: 403

Table 4-217 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-218 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying the version of a specified identity policy

```
GET https://{endpoint}/v5/policies/{policy_id}/versions/{version_id}
```


Example Responses

Status code: 200

Successful

```
{
  "policy_version" : {
    "document" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"*\"]}]}",
    "version_id" : "v1",
    "is_default" : true,
    "created_at" : "2023-09-25T08:00:51.537Z"
  }
}
```

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.6.8 Deleting the Version of a Specified Identity Policy

Function

This API is used to delete a specified version of a specified identity policy. The default identity policy version cannot be deleted.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:policies:deleteVersionV5	Permission_management	policy *	-	-	-

URI

DELETE /v5/policies/{policy_id}/versions/{version_id}

Table 4-219 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
version_id	Yes	String	Identity policy version. The value is a character string starting with **v** and followed by digits, for example, **v5**.

Request Parameters

None

Response Parameters

Status code: 204

Successful

Status code: 403

Table 4-220 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-221 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-222 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Deleting the version of a specified identity policy

```
DELETE https://{endpoint}/v5/policies/{policy_id}/versions/{version_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.6.9 Setting a Specified Identity Policy Version as the Default Version

Function

This API is used to set a specified identity policy version as the default version.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:policies:setDefaultVersionV5	Permission_management	policy *	-	-	-

URI

POST /v5/policies/{policy_id}/versions/{version_id}/set-default

Table 4-223 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
version_id	Yes	String	Identity policy version. The value is a character string starting with **v** and followed by digits, for example, **v5**.

Request Parameters

None

Response Parameters

Status code: 200

Successful

Status code: 403

Table 4-224 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-225 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-226 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Setting a specified identity policy version as the default version

```
POST https://{endpoint}/v5/policies/{policy_id}/versions/{version_id}/set-default
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.7 Managing Permissions

4.1.7.1 Attaching an Identity Policy to an Agency or Trust Agency

Function

This API is used to attach a specified identity policy to a specified agency or trust agency.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:agencies:attachPolicyV5	Permission_management	agency *	g:ResourceTag/<tag-key>	-	-
		-	iam:PolicyURN		

URI

POST /v5/policies/{policy_id}/attach-agency

Table 4-227 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

Table 4-228 Request body parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency or trust agency ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Response Parameters

Status code: 200

Successful

Status code: 403

Table 4-229 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-230 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-231 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Attaching a specified identity policy to agency *xxx*

```
POST https://{endpoint}/v5/policies/{policy_id}/attach-agency

{
  "agency_id" : "xxx"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.7.2 Attaching an Identity Policy to a Group

Function

This API is used to attach a specified identity policy to a specified group.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:groups:attachPolicyV5	Permission_management	group *	-	-	-
		-	iam:PolicyURN		

URI

POST /v5/policies/{policy_id}/attach-group

Table 4-232 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

Table 4-233 Request body parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	Group ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Response Parameters

Status code: 200

Successful

Status code: 403

Table 4-234 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-235 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-236 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Attaching a specified identity policy to group *xxx*

```
POST https://{endpoint}/v5/policies/{policy_id}/attach-group
```



```
{
  "group_id" : "xxx"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.7.3 Attaching an Identity Policy to an IAM User

Function

This API is used to attach a specified identity policy to a specified IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:attachPolicyV5	Permission_management	user *	g:ResourceTag/<tag-key>	-	-
		-	iam:PolicyURN		

URI

POST /v5/policies/{policy_id}/attach-user

Table 4-237 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

Table 4-238 Request body parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Response Parameters

Status code: 200

Successful

Status code: 403

Table 4-239 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-240 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-241 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Attaching a specified identity policy to IAM user *xxx*

```
POST https://{endpoint}/v5/policies/{policy_id}/attach-user

{
  "user_id" : "xxx"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.7.4 Detaching an Identity Policy from an Agency or Trust Agency

Function

This API is used to detach a specified identity policy from a specified agency or trust agency.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:agencies:detachPolicyV5	Permission_management	agency *	g:ResourceTag/<tag-key>	-	-
		-	iam:PolicyURN		

URI

POST /v5/policies/{policy_id}/detach-agency

Table 4-242 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

Table 4-243 Request body parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency or trust agency ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Response Parameters

Status code: 200

Successful

Status code: 403

Table 4-244 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-245 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-246 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Detaching a specified identity policy from agency *xxx*

```
POST https://{endpoint}/v5/policies/{policy_id}/detach-agency

{
  "agency_id" : "xxx"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.7.5 Detaching an Identity Policy from a Group

Function

This API is used to detach a specified identity policy from a specified group.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:groups:detachPolicyV5	Permission_management	group *	-	-	-
		-	iam:PolicyURN		

URI

POST /v5/policies/{policy_id}/detach-group

Table 4-247 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

Table 4-248 Request body parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	Group ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Response Parameters

Status code: 200

Successful

Status code: 403

Table 4-249 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-250 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-251 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Detaching a specified identity policy from group *xxx*

```
POST https://{endpoint}/v5/policies/{policy_id}/detach-group

{
  "group_id" : "xxx"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.7.6 Detaching an Identity Policy from an IAM User

Function

This API is used to detach a specified identity policy from a specified IAM user.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:detachPolicyV5	Permission_management	user *	g:ResourceTag/<tag-key>	-	-
		-	iam:PolicyURN		

URI

POST /v5/policies/{policy_id}/detach-user

Table 4-252 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

Table 4-253 Request body parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Response Parameters

Status code: 200

Successful

Status code: 403

Table 4-254 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-255 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-256 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Detaching a specified identity policy from IAM user *xxx*

```
POST https://{endpoint}/v5/policies/{policy_id}/detach-user

{
  "user_id" : "xxx"
}
```


Example Responses

None

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.7.7 Querying All Entities Attached to a Specified Identity Policy

Function

This API is used to query all entities attached to a specified identity policy.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:policies:listEntitiesV5	List	policy *	-	-	-

URI

GET /v5/policies/{policy_id}/attached-entities

Table 4-257 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Table 4-258 Query Parameters

Parameter	Mandatory	Type	Description
entity_type	No	String	Entity type, which can be **user**, **group**, or **agency**.
limit	No	Integer	Number of records displayed on each page. The value ranges from 1 to 200. The default value is 100. Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Pagination marker. The value contains 4 to 400 characters, including only letters, digits, and the following special characters: +/=-_ Minimum: **4** Maximum: **400**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-259 Response body parameters

Parameter	Type	Description
policy_agencies	Array of **PolicyAgency** objects	Agency and trust agency list.

Parameter	Type	Description
policy_groups	Array of **PolicyGroup** objects	Group list.
policy_users	Array of **PolicyUser** objects	IAM user list.
page_info	**PageInfo** object	Pagination information.

Table 4-260 PolicyAgency

Parameter	Type	Description
agency_id	String	Agency or trust agency ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
attached_at	String	Time when an identity policy is attached.

Table 4-261 PolicyGroup

Parameter	Type	Description
group_id	String	Group ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
attached_at	String	Time when an identity policy is attached.

Table 4-262 PolicyUser

Parameter	Type	Description
user_id	String	IAM user ID.
attached_at	String	Time when an identity policy is attached.

Table 4-263 PageInfo

Parameter	Type	Description
next_marker	String	If this parameter exists, there are subsequent items that are not displayed in the current response body. The value can be used as the pagination marker parameter for the next request to obtain information about the next page. This API can be repeatedly called until this field does not exist.
current_count	Integer	Number of items returned on this page.

Status code: 403

Table 4-264 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-265 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying all entities attached to a specified identity policy

```
GET https://{endpoint}/v5/policies/{policy_id}/attached-entities
```


Example Responses

Status code: 200

Successful


```
{
  "policy_agencies" : [ {
    "agency_id" : "string",
    "attached_at" : "2023-09-25T09:29:06.817Z"
  } ],
  "policy_groups" : [ {
    "group_id" : "string",
    "attached_at" : "2023-09-25T09:29:06.817Z"
  } ],
  "policy_users" : [ {
    "user_id" : "string",
    "attached_at" : "2023-09-25T09:29:06.817Z"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 3
  }
}
```


Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.7.8 Querying All Identity Policies Attached to a Specified Agency or Trust Agency

Function

This API is used to query all identity policies attached to a specified agency or trust agency.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:agencies:listAttachedPoliciesV5	List	agency *	g:ResourceTag/<tag-key>	-	-

URI

GET /v5/agencies/{agency_id}/attached-policies

Table 4-266 Path Parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency or trust agency ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Table 4-267 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The value ranges from 1 to 200. The default value is 100. Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Pagination marker. The value contains 4 to 400 characters, including only letters, digits, and the following special characters: +/=-_ Minimum: **4** Maximum: **400**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-268 Response body parameters

Parameter	Type	Description
attached_policies	Array of **AttachedPolicy** objects	Identity policy list.
page_info	**PageInfo** object	Pagination information.

Table 4-269 AttachedPolicy

Parameter	Type	Description
policy_name	String	Identity policy name. The value contains 1 to 128 characters, including only letters, digits, and the following special characters: _+=.@-
policy_id	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
urn	String	Uniform resource name.
attached_at	String	Time when an identity policy is attached.

Table 4-270 PageInfo

Parameter	Type	Description
next_marker	String	If this parameter exists, there are subsequent items that are not displayed in the current response body. The value can be used as the pagination marker parameter for the next request to obtain information about the next page. This API can be repeatedly called until this field does not exist.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-271 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-272 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-273 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying all identity policies attached to a specified agency

```
GET https://{endpoint}/v5/agencies/{agency_id}/attached-policies
```

Example Responses

Status code: 200

Successful

```
{
  "attached_policies" : [ {
    "policy_name" : "name",
    "policy_id" : "string",
```

```
    "urn" : "iam::accountid:policy:name",
    "attached_at" : "2023-09-25T09:31:44.935Z"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.7.9 Querying All Identity Policies Attached to a Specified Group

Function

This API is used to query all identity policies attached to a specified group.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:groups:listAttachedPoliciesV5	List	group *	-	-	-

URI

GET /v5/groups/{group_id}/attached-policies

Table 4-274 Path Parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	Group ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Table 4-275 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The value ranges from 1 to 200. The default value is 100. Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Pagination marker. The value contains 4 to 400 characters, including only letters, digits, and the following special characters: +/=-_ Minimum: **4** Maximum: **400**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-276 Response body parameters

Parameter	Type	Description
attached_policies	Array of **AttachedPolicy** objects	Identity policy list.
page_info	**PageInfo** object	Pagination information.

Table 4-277 AttachedPolicy

Parameter	Type	Description
policy_name	String	Identity policy name. The value contains 1 to 128 characters, including only letters, digits, and the following special characters: _+=.@-
policy_id	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
urn	String	Uniform resource name.
attached_at	String	Time when an identity policy is attached.

Table 4-278 PageInfo

Parameter	Type	Description
next_marker	String	If this parameter exists, there are subsequent items that are not displayed in the current response body. The value can be used as the pagination marker parameter for the next request to obtain information about the next page. This API can be repeatedly called until this field does not exist.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-279 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-280 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-281 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying all identity policies attached to a specified group

```
GET https://{endpoint}/v5/groups/{group_id}/attached-policies
```

Example Responses

Status code: 200

Successful

```
{
  "attached_policies" : [ {
    "policy_name" : "name",
    "policy_id" : "string",
    "urn" : "iam::accountid:policy:name",
    "attached_at" : "2023-09-25T09:31:44.935Z"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```


Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.7.10 Querying All Identity Policies Attached to a Specified IAM User

Function

This API is used to query all identity policies attached to a specified IAM User.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:users:listAttachedPoliciesV5	List	user *	g:ResourceTag/<tag-key>	-	-

URI

GET /v5/users/{user_id}/attached-policies

Table 4-282 Path Parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	IAM user ID.

Table 4-283 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The value ranges from 1 to 200. The default value is 100. Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Pagination marker. The value contains 4 to 400 characters, including only letters, digits, and the following special characters: +/=-_ Minimum: **4** Maximum: **400**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-284 Response body parameters

Parameter	Type	Description
attached_policies	Array of **AttachedPolicy** objects	Identity policy list.
page_info	**PageInfo** object	Pagination information.

Table 4-285 AttachedPolicy

Parameter	Type	Description
policy_name	String	Identity policy name. The value contains 1 to 128 characters, including only letters, digits, and the following special characters: _+=.@-

Parameter	Type	Description
policy_id	String	Identity policy ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
urn	String	Uniform resource name.
attached_at	String	Time when an identity policy is attached.

Table 4-286 PageInfo

Parameter	Type	Description
next_marker	String	If this parameter exists, there are subsequent items that are not displayed in the current response body. The value can be used as the pagination marker parameter for the next request to obtain information about the next page. This API can be repeatedly called until this field does not exist.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-287 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-288 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-289 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying all identity policies attached to a specified IAM user

```
GET https://{endpoint}/v5/users/{user_id}/attached-policies
```

Example Responses

Status code: 200

Successful

```
{
  "attached_policies" : [ {
    "policy_name" : "name",
    "policy_id" : "string",
    "urn" : "iam::accountid:policy:name",
    "attached_at" : "2023-09-25T09:31:44.935Z"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden

Status Code	Description
404	Not found

Error Codes

See **Error Codes**.

4.1.8 Querying the Authorization Summary

4.1.8.1 Querying the Authorization Summary of a Specified Service

Function

This API is used to query the authorization summary of a specified cloud service.

Authorization Information

No identity policy-based permission required for calling this API.

URI

GET /v5/authorization-schemas/services/{service_code}

Table 4-290 Path Parameters

Parameter	Mandatory	Type	Description
service_code	Yes	String	Abbreviation of a service name. The value contains 1 to 56 characters, including only letters, digits, and hyphens (-).

Request Parameters

None

Response Parameters

Status code: 200

Table 4-291 Response body parameters

Parameter	Type	Description
version	String	Version number of a service authorization summary.
actions	Array of **Action** objects	Action list supported by a cloud service.
resources	Array of **Resource** objects	Resource list supported by a cloud service.
conditions	Array of **Condition** objects	Condition key list supported by a cloud service.
operations	Array of **Operation** objects	Operation list supported by a cloud service.

Table 4-292 Action

Parameter	Type	Description
name	String	Three-segment action name, for example, **iam:policies:createV5"**.
access_level	String	Access level granted when this action is used in a policy.
permission_only	Boolean	Indicates whether this action is used only as a permission and does not correspond to any operation.
description	**Description** object	Description.
aliases	Array of strings	List of action alias, which is used in scenarios where actions are renamed or new actions are split.
resources	Array of **ActionAssociate-dResource** objects	Resource list associated with this action, which is used to define resource-level permissions of this action.
condition_keys	Array of strings	Service-defined condition attributes and some global attributes that are supported by this action and are irrelevant to resources.

Table 4-293 ActionAssociatedResource

Parameter	Type	Description
urn_template	String	Uniform resource name template, which indicates that the uniform resource name of this resource can be used to grant permissions to an action.
required	Boolean	Indicates whether a resource type is mandatory for this action. That is, the action must involve operations on this resource type. For example, **subnet** is a mandatory resource type of **vpc:subnets:get**, and **ou** is an optional resource type of **organizations::tagResource**, because the resource operated by **organizations::tagResource** may also be an account or policy.
condition_keys	Array of strings	Service-defined condition attributes and some global attributes of this action and resource take effect only when this action and resource are matched.

Table 4-294 Resource

Parameter	Type	Description
type_name	String	Resource type name of a cloud service.
urn_template	String	Uniform resource name template, which indicates that the uniform resource name of this resource can be used to grant permissions to an action.

Table 4-295 Condition

Parameter	Type	Description
key	String	Name of a condition key.
value_type	String	Data type of a condition value.
multi_valued	Boolean	Indicates whether a condition value has multiple values.
description	**Description** object	Description.

Table 4-296 Description

Parameter	Type	Description
en_US	String	Description in English. Minimum: **1** Maximum: **1500**
zh_CN	String	Description in Chinese. Minimum: **1** Maximum: **1500**

Table 4-297 Operation

Parameter	Type	Description
operation_id	String	Operation identifier of the OpenAPI. Minimum: **1** Maximum: **64**
operation_action	String	Three-segment action name, for example, **iam:policies:createV5"**.
dependent_actions	Array of strings	Permissions for other actions that may be required for this operation.

Status code: 404

Table 4-298 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying the authorization summary of a specified cloud service

```
GET https://{endpoint}/v5/authorization-schemas/services/{service_code}
```

Example Responses

Status code: 200

Successful


```
{
  "version" : "v1",
  "actions" : [ {
    "name" : "sts:agencies:assume",
    "access_level" : "write",
    "permission_only" : false,
    "description" : {
      "en_US" : "Grants permission to obtain a set of temporary credentials that you can use to access
resources that you might not normally have access to.",
      "zh_CN" : "..."
    },
    "resources" : [ {
      "urn_template" : "iam::<account-id>:agency:<agency-name-with-path>",
      "required" : true
    } ],
    "condition_keys" : [ "sts:ExternalId", "sts:SourceIdentity", "sts:TransitiveTagKeys",
"sts:AgencySessionName" ]
  }, {
    "name" : "sts::getCallerIdentity",
    "access_level" : "read",
    "permission_only" : false,
    "description" : {
      "en_US" : "Grants permission to obtain details about the IAM identity whose credentials are used to call
the API.",
      "zh_CN" : "..."
    }
  }, {
    "name" : "sts::decodeAuthorizationMessage",
    "access_level" : "write",
    "permission_only" : false,
    "description" : {
      "en_US" : "Grants permission to decode additional information about the authorization status of a
request from an encoded message returned in response to a request.",
      "zh_CN" : "..."
    }
  }, {
    "name" : "sts::setSourceIdentity",
    "access_level" : "write",
    "permission_only" : true,
    "description" : {
      "en_US" : "Grants permission to set a source identity on a STS session.",
      "zh_CN" : "..."
    },
    "resources" : [ {
      "urn_template" : "iam::<account-id>:agency:<agency-name-with-path>",
      "required" : true
    } ],
    "condition_keys" : [ "sts:SourceIdentity" ]
  }, {
    "name" : "sts::tagSession",
    "access_level" : "tagging",
    "permission_only" : true,
    "description" : {
      "en_US" : "Grants permission to add tags to a STS session.",
      "zh_CN" : "..."
    },
    "resources" : [ {
      "urn_template" : "iam::<account-id>:agency:<agency-name-with-path>",
      "required" : true
    } ],
    "condition_keys" : [ "sts:TransitiveTagKeys" ]
  } ],
  "resources" : [ {
    "type_name" : "assumed-agency",
    "urn_template" : "sts::<account-id>:assumed-agency:<agency-name>/<session-name>"
  } ],
  "conditions" : [ {
    "key" : "sts:ExternalId",
    "value_type" : "string",
```

```
    "multi_valued" : false,
    "description" : {
      "en_US" : "Filters access by the external ID that is passed in the request.",
      "zh_CN" : "..."
    }
  }, {
    "key" : "sts:SourceIdentity",
    "value_type" : "string",
    "multi_valued" : false,
    "description" : {
      "en_US" : "Filters access by the source identity that is passed in the request.",
      "zh_CN" : "..."
    }
  }, {
    "key" : "sts:TransitiveTagKeys",
    "value_type" : "string",
    "multi_valued" : true,
    "description" : {
      "en_US" : "Filters access by the transitive tag keys that are passed in the request.",
      "zh_CN" : "..."
    }
  }, {
    "key" : "sts:AgencySessionName",
    "value_type" : "string",
    "multi_valued" : false,
    "description" : {
      "en_US" : "Filters access by the agency session name required when you assume an agency.",
      "zh_CN" : "..."
    }
  } ],
  "operations" : [ {
    "operation_id" : "AssumeAgency",
    "operation_action" : "sts:agencies:assume",
    "dependent_actions" : [ "sts::tagSession", "sts::setSourceIdentity" ]
  }, {
    "operation_id" : "GetCallerIdentity",
    "operation_action" : "sts::getCallerIdentity"
  }, {
    "operation_id" : "DecodeAuthorizationMessage",
    "operation_action" : "sts::decodeAuthorizationMessage"
  } ]
}
```


Status Codes

Status Code	Description
200	Successful
404	Not found

Error Codes

See **Error Codes**.

4.1.8.2 Listing Registered Cloud Services

Function

This API is used to list registered cloud services.

Authorization Information

No identity policy-based permission required for calling this API.

URI

GET /v5/authorization-schemas/registered-services

Table 4-299 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The value ranges from 1 to 200. The default value is 100. Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Pagination marker. The value contains 4 to 400 characters, including only letters, digits, and the following special characters: +/=-_ Minimum: **4** Maximum: **400**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-300 Response body parameters

Parameter	Type	Description
service_codes	Array of strings	List of service name abbreviations.
page_info	**PageInfo** object	Pagination information.

Table 4-301 PageInfo

Parameter	Type	Description
next_marker	String	If this parameter exists, there are subsequent items that are not displayed in the current response body. The value can be used as the pagination marker parameter for the next request to obtain information about the next page. This API can be repeatedly called until this field does not exist.
current_count	Integer	Number of items returned on this page.

Example Requests

Listing registered cloud services

```
GET https://{endpoint}/v5/authorization-schemas/registered-services
```

Example Responses

Status code: 200

Successful

```
{
  "service_codes" : [ "service1", "service2" ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 2
  }
}
```

Status Codes

Status Code	Description
200	Successful

Error Codes

See **Error Codes**.

4.1.8.3 Obtaining All Service Principals

Function

This API is used to obtain all service principals.

Authorization Information

No identity policy-based permission required for calling this API.

URI

GET /v5/service-principals

Table 4-302 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The value ranges from 1 to 200. The default value is 100. Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Pagination marker. The value contains 4 to 400 characters, including only letters, digits, and the following special characters: +/=-_ Minimum: **4** Maximum: **400**

Request Parameters

Table 4-303 Request header parameters

Parameter	Mandatory	Type	Description
X-Language	No	String	Language of the returned message. The value can be **zh-cn** or **en-us** and is **zh-cn** by default. Default: **zh-cn**

Response Parameters

Status code: 200

Table 4-304 Response body parameters

Parameter	Type	Description
service_principals	Array of **ServicePrincipal-Metadata** objects	List of service principals.
page_info	**PageInfo** object	Pagination information.

Table 4-305 ServicePrincipalMetadata

Parameter	Type	Description
service_principal	String	Service principal, which starts with **service.** and is followed by a string of 1 to 56 characters containing only letters, digits, and hyphens (-).
service_catalog	String	Cloud service name. Minimum: **1** Maximum: **64**
display_name	String	Service principal name for display.
description	String	Service principal description.

Table 4-306 PageInfo

Parameter	Type	Description
next_marker	String	If this parameter exists, there are subsequent items that are not displayed in the current response body. The value can be used as the pagination marker parameter for the next request to obtain information about the next page. This API can be repeatedly called until this field does not exist.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-307 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Obtaining all service principals

```
GET https://{endpoint}/v5/service-principals
```

Example Responses

Status code: 200

Successful

```
{
  "service_principals" : [ {
    "service_principal" : "service.xxx",
    "service_catalog" : "XXX",
    "display_name" : "display_name",
    "description" : "description"
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful
400	Bad request

Error Codes

See **Error Codes**.

4.1.9 Managing Agencies and Trust Agencies

4.1.9.1 Creating a Service-linked Agency

Function

This API is used to create a service-linked agency.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:agencies:createServiceLinkedAgencyV5	Write	agency *	-	-	-
		-	iam:ServicePrincipal		

URI

PUT /v5/service-linked-agencies

Request Parameters

Table 4-308 Request body parameters

Parameter	Mandatory	Type	Description
service_principal	Yes	String	Service principal, which starts with **service.** and is followed by a string of 1 to 56 characters containing only letters, digits, and hyphens (-).
description	No	String	Description of a service-linked agency. The value cannot contain the following special characters: @#%&<>\$^* Maximum: **1000**

Response Parameters

Status code: 201

Table 4-309 Response body parameters

Parameter	Type	Description
agency	**Agency** object	Agency or trust agency.

Table 4-310 Agency

Parameter	Type	Description
urn	String	Uniform resource name.

Parameter	Type	Description

trust_policy	String	JSON format of the policy document of a trust agency's trust policy. Characters =, <, >, (,), and | are special characters in the grammar and are not included in trust policies.
		The question mark (?) following an element indicates that the element is optional, for example, **sid_block?**.
		The vertical bar (|) separates options, and the parentheses enclose the options, for example, **("Allow" | "Deny")**.
		When an element allows more than one value, use commas (,), and ellipsis (...), for example, **[<policy_statement>, <policy_statement>, ...]**.
		The following listing describes the trust policy language grammar:
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <principal_block>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<principal_block> = ("Principal" | "NotPrincipal") :
		<principal_map>
		
		<principal_map> = { <principal_map_entry>,
		<principal_map_entry>, ... }
		
		<principal_map_entry> = ("IAM" | "Service") :
		[<principal_id_string>, ... |
		<service_principal_string>, ...]
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :

Parameter	Type	Description

		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}
		
		<condition_value_list> = (<condition_value> |
		[<condition_value>, <condition_value>, ...])
		
		<condition_value> = "string"

created_at	String	Time when an agency or trust agency was created.
description	String	Description of an agency or trust agency.
max_session_duration	Integer	Maximum session duration of an agency or trust agency. The default value is 3,600 seconds. The value ranges from 3,600 to 43,200.
path	String	Resource path, which is an empty string by default. It consists of multiple character strings. Each character string must end with a slash (/) and can only contain letters, digits, and the following special characters: .,+@=_-, for example, **foo/bar/**.
agency_id	String	Agency or trust agency ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
agency_name	String	Agency or trust agency name. The value contains 1 to 64 characters, including only letters, digits, and the following special characters: _+=,.@-
trust_domain_id	String	Delegated account ID, which is only in agencies but not in trust agencies.
trust_domain_name	String	Delegated account name, which is only in agencies but not in trust agencies.

Status code: 403

Table 4-311 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-312 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-313 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Creating a service-linked agency whose service principal is *service.xxx*

```
PUT https://{endpoint}/v5/service-linked-agencies

{
  "service_principal" : "service.xxx",
  "description" : "description"
}
```

Example Responses

Status code: 201

Successful


```
{
  "agency" : {
    "urn" : "iam::accountid:agency:service-linked-agency/service.xxx/name",
    "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Action\":[\"sts:agencies:assume\",\"sts::tagSession
\",\"sts::setSourceIdentity\"],\"Effect\":\"Allow\",\"Principal\":{\"Service\":[\"service.xxx\"]}}]}",
    "created_at" : "2023-09-11T10:13:25.414Z",
    "description" : "description",
    "max_session_duration" : 3600,
    "path" : "service-linked-agency/service.xxx/",
    "agency_id" : "id",
    "agency_name" : "name",
    "trust_domain_id" : null,
    "trust_domain_name" : null
  }
}
```


Status Codes

Status Code	Description
201	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.9.2 Deleting a Service-linked Agency

Function

This API is used to delete a service-linked agency.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:agencies:deleteServiceLinkedAgencyV5	Write	agency *	g:ResourceTag/<tag-key>	-	-

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
		-	iam:ServicePrincipal		

URI

DELETE /v5/service-linked-agencies/{agency_id}

Table 4-314 Path Parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency or trust agency ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

None

Response Parameters

Status code: 202

Table 4-315 Response body parameters

Parameter	Type	Description
deletion_task_id	String	ID of a deleted task.

Status code: 403

Table 4-316 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-317 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-318 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Deleting a service-linked agency

```
DELETE https://{endpoint}/v5/service-linked-agencies/{agency_id}
```

Example Responses

Status code: 202

Successful

```
{
  "deletion_task_id" : "task"
}
```

Status Codes

Status Code	Description
202	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.9.3 Obtaining the Deletion Status of a Service-linked Agency

Function

This API is used to obtain the deletion status of a service-linked agency.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:agencies:getServiceLinkedAgencyDeletionStatusV5	Read	agency *	-	-	-

URI

GET /v5/service-linked-agencies/deletion-task/{deletion_task_id}

Table 4-319 Path Parameters

Parameter	Mandatory	Type	Description
deletion_task_id	Yes	String	ID of a deleted task. Minimum: **1** Maximum: **1000**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-320 Response body parameters

Parameter	Type	Description
status	String	Status of a deleted task.
reason	String	Cause of the deletion failure.
agency_usage_list	Array of **AgencyUsage** objects	List of scenarios where a service-linked agency is being used

Table 4-321 AgencyUsage

Parameter	Type	Description
region	String	Region name.
resources	Array of strings	Uniform resource name list.

Status code: 403

Table 4-322 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-323 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Obtaining the deletion status of a service-linked agency

```
GET https://{endpoint}/v5/service-linked-agencies/deletion-task/{deletion_task_id}
```

Example Responses

Status code: 200

Successful

```
{
  "status" : "succeeded"
}
```

Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.9.4 Listing Agencies and Trust Agencies Based on Specified Conditions

Function

This API is used to list agencies and trust agencies based on specified conditions.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:agencies:listV5	List	agency *	-	-	-

URI

GET /v5/agencies

Table 4-324 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. The value ranges from 1 to 200. The default value is 100. Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Pagination marker. The value contains 4 to 400 characters, including only letters, digits, and the following special characters: +/=-_ Minimum: **4** Maximum: **400**

Parameter	Mandatory	Type	Description
path_prefix	No	String	Resource path prefix, which consists of multiple character strings. Each character string must end with a slash (/) and can only contain letters, digits, and the following special characters: .,+@=_-, for example, **foo/bar/**. Maximum: **512**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-325 Response body parameters

Parameter	Type	Description
agencies	Array of **Agency** objects	Agency and trust agency list.
page_info	**PageInfo** object	Pagination information.

Table 4-326 Agency

Parameter	Type	Description
urn	String	Uniform resource name.

Parameter	Type	Description

trust_policy	String	JSON format of the policy document of a trust agency's trust policy. Characters =, <, >, (,), and | are special characters in the grammar and are not included in trust policies.
		The question mark (?) following an element indicates that the element is optional, for example, **sid_block?**.
		The vertical bar (|) separates options, and the parentheses enclose the options, for example, **("Allow" | "Deny")**.
		When an element allows more than one value, use commas (,), and ellipsis (...), for example, **[<policy_statement>, <policy_statement>, ...]**.
		The following listing describes the trust policy language grammar:
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <principal_block>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<principal_block> = ("Principal" | "NotPrincipal") :
		<principal_map>
		
		<principal_map> = { <principal_map_entry>,
		<principal_map_entry>, ... }
		
		<principal_map_entry> = ("IAM" | "Service") :
		[<principal_id_string>, ... |
		<service_principal_string>, ...]
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :

Parameter	Type	Description

		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}
		
		<condition_value_list> = (<condition_value> |
		[<condition_value>, <condition_value>, ...])
		
		<condition_value> = "string"

created_at	String	Time when an agency or trust agency was created.
description	String	Description of an agency or trust agency.
max_session_duration	Integer	Maximum session duration of an agency or trust agency. The default value is 3,600 seconds. The value ranges from 3,600 to 43,200.
path	String	Resource path, which is an empty string by default. It consists of multiple character strings. Each character string must end with a slash (/) and can only contain letters, digits, and the following special characters: .,+@=_-, for example, **foo/bar/**.
agency_id	String	Agency or trust agency ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
agency_name	String	Agency or trust agency name. The value contains 1 to 64 characters, including only letters, digits, and the following special characters: _+=,.@-
trust_domain_id	String	Delegated account ID, which is only in agencies but not in trust agencies.
trust_domain_name	String	Delegated account name, which is only in agencies but not in trust agencies.

Table 4-327 PageInfo

Parameter	Type	Description
next_marker	String	If this parameter exists, there are subsequent items that are not displayed in the current response body. The value can be used as the pagination marker parameter for the next request to obtain information about the next page. This API can be repeatedly called until this field does not exist.
current_count	Integer	Number of items returned on this page.

Status code: 403

Table 4-328 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Example Requests

Listing All Agencies and Trust Agencies

```
GET https://{endpoint}/v5/agencies
```

Example Responses

Status code: 200

Successful

```
{
  "agencies" : [ {
    "urn" : "iam::accountid:agency:name",
    "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Action\":[\"sts:agencies:assume\",\"sts::tagSession
\",\"sts::setSourceIdentity\"],\"Effect\":\"Allow\",\"Principal\":{\"IAM\":[\"xxx\"]}}]}",
    "created_at" : "2023-09-21T01:17:19.590Z",
    "description" : "description",
    "max_session_duration" : 3600,
    "path" : "",
    "agency_id" : "string",
```



```
    "agency_name" : "name",
    "trust_domain_id" : null,
    "trust_domain_name" : null
  } ],
  "page_info" : {
    "next_marker" : "marker",
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful
403	Forbidden

Error Codes

See **Error Codes**.

4.1.9.5 Creating a Trust Agency

Function

This API is used to create a trust agency.

NOTE

Trust agencies can only have identity policies attached, and are only compatible with cloud services that support identity policies. For details, see "Cloud Services for Using Identity Policies and Trust Agencies" in the *Identity and Access Management User Guide*.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:agencies:createV5	Write	agency *	-	-	-

URI

POST /v5/agencies

Request Parameters

Table 4-329 Request body parameters

Parameter	Mandatory	Type	Description
agency_name	Yes	String	Trust agency name. The value can contain 1 to 64 characters. Only letters, digits, hyphens (-), and the following special characters are allowed: _+=,.@
path	No	String	Resource path, which is an empty string by default. It consists of multiple character strings. Each character string must end with a slash (/) and can only contain letters, digits, and the following special characters: .,+@=_-, for example, **foo/bar/**.

Parameter	Mandatory	Type	Description

trust_policy	Yes	String	JSON format of the policy document of a trust agency's trust policy. Characters =, <, >, (,), and | are special characters in the grammar and are not included in trust policies.
			The question mark (?) following an element indicates that the element is optional, for example, **sid_block?**.
			The vertical bar (|) separates options, and the parentheses enclose the options, for example, **("Allow" | "Deny")**.
			When an element allows more than one value, use commas (,), and ellipsis (...), for example, **[<policy_statement>, <policy_statement>, ...]**.
			The following listing describes the trust policy language grammar:
			policy = {
			  <version_block>,
			  <statement_block>
			}
			
			<version_block> = "Version" : ("5.0")
			
			<statement_block> = "Statement" :
			[<policy_statement>,
			<policy_statement>, ...]
			
			<policy_statement> = {
			  <sid_block?>,
			  <principal_block>,
			  <effect_block>,
			  <action_block>,
			  <resource_block?>,
			  <condition_block?>
			}
			
			<sid_block> = "Sid" : <sid_string>
			
			<principal_block> = ("Principal" |
			"NotPrincipal") : <principal_map>
			
			<principal_map> =
			{ <principal_map_entry>,
			<principal_map_entry>, ... }
			
			<principal_map_entry> = ("IAM" |
			"Service") : [<principal_id_string>, ... |
			<service_principal_string>, ...]
			
			<effect_block> = "Effect" : ("Allow" |

Parameter	Mandatory	Type	Description

			"Deny")
			
			<action_block> = ("Action" |
			"NotAction") : [<action_string>,
			<action_string>, ...]
			
			<resource_block> = ("Resource" |
			"NotResource") : [<resource_string>,
			<resource_string>, ...]
			
			<condition_block> = "Condition" :
			{ <condition_map> }
			
			<condition_map> = {
			  <condition_type_string> :
			{ <condition_key_string> :
			<condition_value_list> },
			  <condition_type_string> :
			{ <condition_key_string> :
			<condition_value_list> },
			  ...
			}
			
			<condition_value_list> =
			(<condition_value> |
			[<condition_value>,
			<condition_value>, ...])
			
			<condition_value> = "string"

max_session_duration	No	Integer	Maximum session duration of a trust agency. The value ranges from 3,600 to 43,200. The default value is 3,600 seconds.
description	No	String	Description of the trust agency. The value is a string that can contain up to 1,000 characters. By default, the value is an empty string. Maximum: **1000**

Response Parameters

Status code: 201

Table 4-330 Response body parameters

Parameter	Type	Description
agency	**TrustAgency** object	Trust agency.

Table 4-331 TrustAgency

Parameter	Type	Description
urn	String	Uniform resource name.

Parameter	Type	Description

trust_policy	String	JSON format of the policy document of a trust agency's trust policy. Characters =, <, >, (,), and | are special characters in the grammar and are not included in trust policies.
		The question mark (?) following an element indicates that the element is optional, for example, **sid_block?**.
		The vertical bar (|) separates options, and the parentheses enclose the options, for example, **("Allow" | "Deny")**.
		When an element allows more than one value, use commas (,), and ellipsis (...), for example, **[<policy_statement>, <policy_statement>, ...]**.
		The following listing describes the trust policy language grammar:
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <principal_block>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<principal_block> = ("Principal" | "NotPrincipal") :
		<principal_map>
		
		<principal_map> = { <principal_map_entry>,
		<principal_map_entry>, ... }
		
		<principal_map_entry> = ("IAM" | "Service") :
		[<principal_id_string>, ... |
		<service_principal_string>, ...]
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :

Parameter	Type	Description

		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}
		
		<condition_value_list> = (<condition_value> |
		[<condition_value>, <condition_value>, ...])
		
		<condition_value> = "string"

created_at	String	Time when a trust agency is created.
description	String	Description of a trust agency.
max_session_duration	Integer	Maximum session duration of a trust agency. The value ranges from 3,600 to 43,200. The default value is 3,600 seconds.
path	String	Resource path, which is an empty string by default. It consists of multiple character strings. Each character string must end with a slash (/) and can only contain letters, digits, and the following special characters: .,+@=_-, for example, **foo/bar/**.
agency_id	String	Trust agency ID. The value must contain 1 to 64 characters. Only letters, digits, and hyphens (-) are allowed.
agency_name	String	Trust agency name. The value can contain 1 to 64 characters. Only letters, digits, hyphens (-), and the following special characters are allowed: _+=,.@
trust_domain_id	String	Delegated account ID, which is only in agencies but not in trust agencies.
trust_domain_name	String	Delegated account name, which is only in agencies but not in trust agencies.

Status code: 400

Table 4-332 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-333 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 409

Table 4-334 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Creating a trust agency **name**

```
POST https://{endpoint}/v5/agencies

{
  "agency_name" : "name",
  "path" : "",
  "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Action\":[\"sts:agencies:assume\",\"sts::tagSession
\",\"sts::setSourceIdentity\"],\"Effect\":\"Allow\",\"Principal\":{\"IAM\":[\"xxx\"]}}]}",
  "max_session_duration" : 3600,
  "description" : "description"
}
```


Example Responses

Status code: 201

Successful


```
{
  "agency" : {
    "urn" : "iam::accountid:agency:name",
    "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Action\":[\"sts:agencies:assume\",\"sts::tagSession
\",\"sts::setSourceIdentity\"],\"Effect\":\"Allow\",\"Principal\":{\"IAM\":[\"xxx\"]}}]}",
    "created_at" : "2023-09-21T01:17:19.590Z",
    "description" : "description",
    "max_session_duration" : 3600,
    "path" : "",
    "agency_id" : "string",
    "agency_name" : "name",
    "trust_domain_id" : null,
    "trust_domain_name" : null
  }
}
```


Status Codes

Status Code	Description
201	Successful
400	Bad request
403	Forbidden
409	Conflict

Error Codes

See **Error Codes**.

4.1.9.6 Querying Agency or Trust Agency Details

Function

This API is used to query agency or trust agency details.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:agencies:getV5	Read	agency *	g:ResourceTag/<tag-key>	-	-

URI

GET /v5/agencies/{agency_id}

Table 4-335 Path Parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Agency or trust agency ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).

Request Parameters

None

Response Parameters

Status code: 200

Table 4-336 Response body parameters

Parameter	Type	Description
agency	**AgencyEx** object	Agency or trust agency.

Table 4-337 AgencyEx

Parameter	Type	Description
urn	String	Uniform resource name.

Parameter	Type	Description

trust_policy	String	JSON format of the policy document of a trust agency's trust policy. Characters =, <, >, (,), and | are special characters in the grammar and are not included in trust policies.
		The question mark (?) following an element indicates that the element is optional, for example, **sid_block?**.
		The vertical bar (|) separates options, and the parentheses enclose the options, for example, **("Allow" | "Deny")**.
		When an element allows more than one value, use commas (,), and ellipsis (...), for example, **[<policy_statement>, <policy_statement>, ...]**.
		The following listing describes the trust policy language grammar:
		policy = {
		  <version_block>,
		  <statement_block>
		}
		
		<version_block> = "Version" : ("5.0")
		
		<statement_block> = "Statement" :
		[<policy_statement>, <policy_statement>, ...]
		
		<policy_statement> = {
		  <sid_block?>,
		  <principal_block>,
		  <effect_block>,
		  <action_block>,
		  <resource_block?>,
		  <condition_block?>
		}
		
		<sid_block> = "Sid" : <sid_string>
		
		<principal_block> = ("Principal" | "NotPrincipal") :
		<principal_map>
		
		<principal_map> = { <principal_map_entry>,
		<principal_map_entry>, ... }
		
		<principal_map_entry> = ("IAM" | "Service") :
		[<principal_id_string>, ... |
		<service_principal_string>, ...]
		
		<effect_block> = "Effect" : ("Allow" | "Deny")
		
		<action_block> = ("Action" | "NotAction") :
		[<action_string>, <action_string>, ...]
		
		<resource_block> = ("Resource" | "NotResource") :
		[<resource_string>, <resource_string>, ...]
		
		<condition_block> = "Condition" :

Parameter	Type	Description

		{ <condition_map> }
		
		<condition_map> = {
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  <condition_type_string> :
		{ <condition_key_string> : <condition_value_list> },
		  ...
		}
		
		<condition_value_list> = (<condition_value> |
		[<condition_value>, <condition_value>, ...])
		
		<condition_value> = "string"

created_at	String	Time when an agency or trust agency was created.
description	String	Description of an agency or trust agency.
max_session_duration	Integer	Maximum session duration of an agency or trust agency. The default value is 3,600 seconds. The value ranges from 3,600 to 43,200.
path	String	Resource path, which is an empty string by default. It consists of multiple character strings. Each character string must end with a slash (/) and can only contain letters, digits, and the following special characters: .,+@=_-, for example, **foo/bar/**.
agency_id	String	Agency or trust agency ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
agency_name	String	Agency or trust agency name. The value contains 1 to 64 characters, including only letters, digits, and the following special characters: _+=,.@-
trust_domain_id	String	Delegated account ID, which is only in agencies but not in trust agencies.
trust_domain_name	String	Delegated account name, which is only in agencies but not in trust agencies.
tags	Array of **Tag** objects	List of custom tags.

Table 4-338 Tag

Parameter	Type	Description
tag_key	String	Tag key. The value can contain 1 to 64 characters. Letters, digits, spaces, and the following special characters are allowed: _.:=+-@. The key cannot start with a space or _**sys**_ or end with a space. Minimum: **1** Maximum: **64**
tag_value	String	Tag value. The value can be an empty string or contain 0 to 128 characters. Letters, digits, spaces, and the following special characters are allowed: _.:/=+-@ Minimum: **0** Maximum: **128**

Status code: 403

Table 4-339 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-340 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Querying agency details

```
GET https://{endpoint}/v5/agencies/{agency_id}
```

Example Responses

Status code: 200

Successful


```
{
  "agency" : {
    "urn" : "iam::accountid:agency:name",
    "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Action\":[\"sts:agencies:assume\",\"sts::tagSession
\",\"sts::setSourceIdentity\"],\"Effect\":\"Allow\",\"Principal\":{\"IAM\":[\"xxx\"]}}]}",
    "created_at" : "2023-09-21T01:17:19.590Z",
    "description" : "description",
    "max_session_duration" : 3600,
    "path" : "",
    "agency_id" : "string",
    "agency_name" : "name",
    "trust_domain_id" : null,
    "trust_domain_name" : null,
    "tags" : [ {
      "tag_key" : "key",
      "tag_value" : "value"
    } ]
  }
}
```


Status Codes

Status Code	Description
200	Successful
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.1.9.7 Modifying a Trust Agency

Function

This API is used to modify a trust agency.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:agencies:updateV5	Write	agency *	g:ResourceTag/<tag-key>	-	-

URI

PUT /v5/agencies/{agency_id}

Table 4-341 Path Parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Trust agency ID. The value must contain 1 to 64 characters. Only letters, digits, and hyphens (-) are allowed.

Request Parameters

Table 4-342 Request body parameters

Parameter	Mandatory	Type	Description
max_session_duration	No	Integer	Maximum session duration of a trust agency. The value ranges from 3,600 to 43,200. The default value is 3,600 seconds.
description	No	String	Description of a trust agency. Maximum: **1000**

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-343 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 403

Table 4-344 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-345 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-346 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Modifying a trust agency


```
PUT https://{endpoint}/v5/agencies/{agency_id}

{
  "max_session_duration" : 3600,
  "description" : "description"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.9.8 Deleting a Trust Agency

Function

This API is used to delete a trust agency.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:agencies:deleteV5	Write	agency *	g:ResourceTag/<tag-key>	-	-

URI

DELETE /v5/agencies/{agency_id}

Table 4-347 Path Parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Trust agency ID. The value must contain 1 to 64 characters. Only letters, digits, and hyphens (-) are allowed.

Request Parameters

None

Response Parameters

Status code: 204

Successful

Status code: 403

Table 4-348 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-349 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-350 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Deleting a trust agency

```
DELETE https://{endpoint}/v5/agencies/{agency_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	Successful
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.9.9 Modifying the Trust Policy of a Trust Agency

Function

This API is used to modify the trust policy of a trust agency.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam:agencies:updateTrustPolicyV5	Write	agency *	g:ResourceTag/<tag-key>	-	-

URI

PUT /v5/agencies/{agency_id}/trust-policy

Table 4-351 Path Parameters

Parameter	Mandatory	Type	Description
agency_id	Yes	String	Trust agency ID. The value must contain 1 to 64 characters. Only letters, digits, and hyphens (-) are allowed.

Request Parameters

Table 4-352 Request body parameters

Parameter	Mandatory	Type	Description

trust_policy	Yes	String	JSON format of the policy document of a trust agency's trust policy. Characters =, <, >, (,), and | are special characters in the grammar and are not included in trust policies.
			The question mark (?) following an element indicates that the element is optional, for example, **sid_block?**.
			The vertical bar (|) separates options, and the parentheses enclose the options, for example, **("Allow" | "Deny")**.
			When an element allows more than one value, use commas (,), and ellipsis (...), for example, **[<policy_statement>, <policy_statement>, ...]**.
			The following listing describes the trust policy language grammar:
			policy = {
			  <version_block>,
			  <statement_block>
			}
			
			<version_block> = "Version" : ("5.0")
			
			<statement_block> = "Statement" :
			[<policy_statement>,
			<policy_statement>, ...]
			
			<policy_statement> = {
			  <sid_block?>,
			  <principal_block>,
			  <effect_block>,
			  <action_block>,
			  <resource_block?>,
			  <condition_block?>
			}
			
			<sid_block> = "Sid" : <sid_string>
			
			<principal_block> = ("Principal" |
			"NotPrincipal") : <principal_map>
			
			<principal_map> =
			{ <principal_map_entry>,
			<principal_map_entry>, ... }

Parameter	Mandatory	Type	Description

			<principal_map_entry> = ("IAM" | "Service") : [<principal_id_string>, ... | <service_principal_string>, ...]
			
			<effect_block> = "Effect" : ("Allow" | "Deny")
			
			<action_block> = ("Action" | "NotAction") : [<action_string>, <action_string>, ...]
			
			<resource_block> = ("Resource" | "NotResource") : [<resource_string>, <resource_string>, ...]
			
			<condition_block> = "Condition" : { <condition_map> }
			
			<condition_map> = {
			  <condition_type_string> : { <condition_key_string> : <condition_value_list> },
			  <condition_type_string> : { <condition_key_string> : <condition_value_list> },
			  ...
			}
			
			<condition_value_list> = (<condition_value> | [<condition_value>, <condition_value>, ...])
			
			<condition_value> = "string"

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-353 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-354 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-355 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-356 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Modifying the trust policy of a trust agency

```
PUT https://{endpoint}/v5/agencies/{agency_id}/trust-policy

{
  "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Action\":[\"sts:agencies:assume\",\"sts::tagSession
\",\"sts::setSourceIdentity\"],\"Effect\":\"Allow\",\"Principal\":{\"IAM\":[\"xxx\"]}}]}"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.10 Managing Account Functions

4.1.10.1 Obtaining the Summary of the Usage and Quota of IAM Entities in an Account

Function

This API is used to obtain the summary of the usage and quota of IAM entities in an account.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam::getAccountSummaryV5	List	-	-	-	-

URI

GET /v5/account-summary

Request Parameters

None

Response Parameters

Status code: 200

Table 4-357 Response body parameters

Parameter	Type	Description
attached_policies_per_agency_quota	Integer	Maximum number of identity policies that can be attached to an agency or trust agency.
attached_policies_per_group_quota	Integer	Maximum number of identity policies that can be attached to a group.
attached_policies_per_user_quota	Integer	Maximum number of identity policies that can be attached to an IAM user.
policies_quota	Integer	Maximum number of custom identity policies.
policy_size_quota	Integer	Maximum characters in the policy documents of identity and trust policies, excluding spaces.
versions_per_policy_quota	Integer	Maximum number of versions that can be retained for a custom identity policy at a time.
policies	Integer	Number of custom identity policies created by the account.
agencies	Integer	Total number of agencies and trust agencies created by the account.
agencies_quota	Integer	Maximum number of agencies and trust agencies that can be created by the account.
users	Integer	Number of IAM users created by the account, including the root user.
users_quota	Integer	Maximum number of IAM users that can be created by the account, including the root user.
groups	Integer	Number of groups created by the account.
groups_quota	Integer	Maximum number of groups that can be created by the account.
root_user_mfa_enabled	Integer	Number of enabled MFA devices bound to the root user.

Status code: 404

Table 4-358 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Obtaining the summary of the usage and quota of IAM entities in an account

```
GET https://{endpoint}/v5/account-summary
```

Example Responses

Status code: 200

Successful

```
{
  "attached_policies_per_agency_quota" : 10,
  "attached_policies_per_group_quota" : 10,
  "attached_policies_per_user_quota" : 10,
  "policies_quota" : 1500,
  "policy_size_quota" : 6144,
  "versions_per_policy_quota" : 5,
  "policies" : 133,
  "agencies" : 50,
  "agencies_quota" : 50,
  "users" : 135,
  "users_quota" : 500,
  "groups" : 34,
  "groups_quota" : 500,
  "root_user_mfa_enabled" : 0
}
```

Status Codes

Status Code	Description
200	Successful
404	Not found

Error Codes

See **Error Codes**.

4.1.10.2 Obtaining the Function Status of an Account

Function

This API is used to obtain the function status of an account.

Authorization Information

No identity policy-based permission required for calling this API.

URI

GET /v5/features/{feature_name}

Table 4-359 Path Parameters

Parameter	Mandatory	Type	Description
feature_name	Yes	String	Unique name of a function feature. Minimum: **1** Maximum: **36**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-360 Response body parameters

Parameter	Type	Description
feature_status	String	Function status.

Example Requests

Obtaining the specified function status of an account

```
GET https://{endpoint}/v5/features/{feature_name}
```

Example Responses

Status code: 200

Successful


```
{
  "feature_status" : "on"
}
```

Status Codes

Status Code	Description
200	Successful

Error Codes

See **Error Codes**.

4.1.10.3 Enabling or Disabling the Asymmetric Signature for an Account

Function

This API is used to enable or disable the asymmetric signature for an account.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam::setAsymmetricSignatureSwitchV5	Write	-	-	-	-

URI

PUT /v5/asymmetric-signature-switch

Request Parameters

Table 4-361 Request body parameters

Parameter	Mandatory	Type	Description
asymmetric_signature	Yes	**AsymmetricSignature** object	Whether the asymmetric signature is enabled for an account.

Table 4-362 AsymmetricSignature

Parameter	Mandatory	Type	Description
asymmetric_signature_switch	Yes	Boolean	Asymmetric signature switch.

Response Parameters

Status code: 204

Successful

Status code: 403

Table 4-363 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Example Requests

Enabling the asymmetric signature for an account

```
PUT https://{endpoint}/v5/asymmetric-signature-switch

{
  "asymmetric_signature" : {
    "asymmetric_signature_switch" : true
  }
}
```

Example Responses

None

Status Codes

Status Code	Description
204	Successful
403	Forbidden

Error Codes

See **Error Codes**.

4.1.10.4 Obtaining the Asymmetric Signature Switch Status of an Account

Function

This API is used to obtain the asymmetric signature switch status of an account.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam::getAsymmetricSignatureSwitchV5	Read	-	-	-	-

URI

GET /v5/asymmetric-signature-switch

Request Parameters

None

Response Parameters

Status code: 200

Table 4-364 Response body parameters

Parameter	Type	Description
asymmetric_signature	**AsymmetricSignatureWithDomainId** object	Asymmetric signature switch of an account.

Table 4-365 AsymmetricSignatureWithDomainId

Parameter	Type	Description
domain_id	String	Account ID.
asymmetric_signature_switch	Boolean	Asymmetric signature switch.

Status code: 403

Table 4-366 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Example Requests

Obtaining the asymmetric signature switch status of an account

```
GET https://{endpoint}/v5/asymmetric-signature-switch
```

Example Responses

Status code: 200

Successful

```
{
  "asymmetric_signature" : {
    "asymmetric_signature_switch" : true,
    "domain_id" : "xxxxx"
  }
}
```


Status Codes

Status Code	Description
200	Successful
403	Forbidden

Error Codes

See **Error Codes**.

4.1.11 Managing Resource Tags

4.1.11.1 Adding Tags to IAM Resources

Function

This API is used to add tags to IAM resources.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam::tagForResourceV5	Tagging	agency	g:ResourceTag/<tag-key>	-	-
		user	g:ResourceTag/<tag-key>		
		-	• g:RequestTag/<tag-key> • g:TagKeys		

URI

POST /v5/{resource_type}/{resource_id}/tags/create

Table 4-367 Path Parameters

Parameter	Mandatory	Type	Description
resource_id	Yes	String	Resource ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
resource_type	Yes	String	Resource type. The value can be **trust agency** or **user**.

Request Parameters

Table 4-368 Request body parameters

Parameter	Mandatory	Type	Description
tags	No	Array of **Tag** objects	List of custom tags. Array Length: **1 - 20**

Table 4-369 Tag

Parameter	Mandatory	Type	Description
tag_key	Yes	String	Tag key. The value can contain 1 to 64 characters. Letters, digits, spaces, and the following special characters are allowed: _.:=+-@. The key cannot start with a space or _**sys**_ or end with a space. Minimum: **1** Maximum: **64**
tag_value	Yes	String	Tag value. The value can be an empty string or contain 0 to 128 characters. Letters, digits, spaces, and the following special characters are allowed: _.:/=+-@ Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 4-370 Response body parameters

Parameter	Type	Description
tags	Array of **Tag** objects	List of custom tags.

Table 4-371 Tag

Parameter	Type	Description
tag_key	String	Tag key. The value can contain 1 to 64 characters. Letters, digits, spaces, and the following special characters are allowed: _.:=+-@. The key cannot start with a space or _**sys**_ or end with a space. Minimum: **1** Maximum: **64**
tag_value	String	Tag value. The value can be an empty string or contain 0 to 128 characters. Letters, digits, spaces, and the following special characters are allowed: _.:/=+-@ Minimum: **0** Maximum: **128**

Status code: 400

Table 4-372 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-373 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Parameter	Type	Description
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-374 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-375 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Adding a tag to a specified IAM resource, with tag key **key** and tag value **value**

```
POST https://{endpoint}/v5/{resource_type}/{resource_id}/tags/create

{
  "tags" : [ {
    "tag_key" : "key",
    "tag_value" : "value"
  } ]
}
```

Example Responses

Status code: 200

Successful

```
{
  "tags" : [ {
```

```
  "tag_key" : "key",
  "tag_value" : "value"
 } ]
}
```

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.11.2 Deleting Some Tags of a Specified Resource

Function

This API is used to delete some tags of a specified resource.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam::untagForResourceV5	Tagging	agency	g:ResourceTag/<tag-key>	-	-
		user	g:ResourceTag/<tag-key>		
		-	• g:RequestTag/<tag-key> • g:TagKeys		

URI

DELETE /v5/{resource_type}/{resource_id}/tags/delete

Table 4-376 Path Parameters

Parameter	Mandatory	Type	Description
resource_id	Yes	String	Resource ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
resource_type	Yes	String	Resource type. The value can be **trust agency** or **user**.

Request Parameters

Table 4-377 Request body parameters

Parameter	Mandatory	Type	Description
[items]	No	Array of strings	Tag keys to be deleted. Array Length: **1 - 20**

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-378 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-379 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-380 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Status code: 409

Table 4-381 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Deleting two tags of a specified resource, whose tag keys are **key1** and **key2** respectively

```
DELETE https://{endpoint}/v5/{resource_type}/{resource_id}/tags/delete

[ "key1", "key2" ]
```

Example Responses

None

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.1.11.3 Obtaining All Tags of a Specified Resource

Function

This API is used to obtain all tags of a specified resource.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
iam::listTagsForResourceV5	List	agency	g:ResourceTag/<tag-key>	-	-
		user	g:ResourceTag/<tag-key>		

URI

GET /v5/{resource_type}/{resource_id}/tags

Table 4-382 Path Parameters

Parameter	Mandatory	Type	Description
resource_id	Yes	String	Resource ID. The value contains 1 to 64 characters, including only letters, digits, and hyphens (-).
resource_type	Yes	String	Resource type. The value can be **trust agency** or **user**.

Request Parameters

None

Response Parameters

Status code: 200

Table 4-383 Response body parameters

Parameter	Type	Description
tags	Array of **Tag** objects	List of custom tags.

Table 4-384 Tag

Parameter	Type	Description
tag_key	String	Tag key. The value can contain 1 to 64 characters. Letters, digits, spaces, and the following special characters are allowed: _.:=+-@. The key cannot start with a space or _**sys**_ or end with a space. Minimum: **1** Maximum: **64**
tag_value	String	Tag value. The value can be an empty string or contain 0 to 128 characters. Letters, digits, spaces, and the following special characters are allowed: _.:/=+-@ Minimum: **0** Maximum: **128**

Status code: 403

Table 4-385 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-386 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Example Requests

Obtaining all tags of a specified resource

```
GET https://{endpoint}/v5/{resource_type}/{resource_id}/tags
```

Example Responses

Status code: 200

Successful

```
{
  "tags" : [ {
    "tag_key" : "key",
    "tag_value" : "value"
  } ]
}
```

Status Codes

Status Code	Description
200	Successful

Status Code	Description
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.2 STS

4.2.1 Temporary security credentials

4.2.1.1 Obtaining a Temporary Security Credential Through an Agency or Trust Agency

Function

This API is used to obtain a temporary security credential through an agency or trust agency. The temporary security credential can be used to control access to cloud resources.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
sts:agencies:assume	Write	agency *	g:ResourceTag/<tag-key>	-	• sts::tagSession • sts::setSourceIdentity

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
		-	• sts:ExternalId • sts:SourceIdentity • sts:TransitiveTagKeys • sts:AgencySessionName • g:RequestTag/<tag-key> • g:TagKeys • g:SourceAccount • g:SourceUrn		

URI

POST /v5/agencies/assume

Request Parameters

Table 4-387 Request header parameters

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	When an API is called using a temporary security credential, the HTTP request header **X-Security-Token** must be provided. The value is the **security_token** field of the temporary security credential.

Table 4-388 Request body parameters

Parameter	Mandatory	Type	Description
duration_seconds	No	Integer	Validity period (in seconds) of the obtained temporary security credential. Note that the duration must be less than the maximum session duration set for the agency and cannot exceed 3600 seconds when the **X-Security-Token** header is carried. Minimum: **900** Maximum: **43200** Default: **3600**
external_id	No	String	External ID to prevent confused deputy problem. Minimum: **2** Maximum: **1224**
policy	No	String	Custom policy. The permission scope of the temporary security credential obtained in this session cannot exceed the permissions specified in the custom policy. Minimum: **2** Maximum: **2048**
policy_ids	No	Array of strings	Predefined policy list. The permission scope of the temporary security credential obtained in this session cannot exceed the permissions specified in the predefined policy. Maximum: **64**
agency_urn	Yes	String	URN of a target agency. Maximum: **1500**
agency_session_name	Yes	String	Name of the assumed-agency session. Minimum: **2** Maximum: **128**

Parameter	Mandatory	Type	Description
serial_number	No	String	Serial number of the virtual MFA device bound to a caller. Minimum: **9** Maximum: **256**
token_code	No	String	6-digit code of the virtual MFA device bound to a caller. Minimum: **6** Maximum: **6**
source_identity	No	String	Identity declared by the initial caller in the call chain. Minimum: **2** Maximum: **64**
tags	No	Array of **TagDto** objects	List of custom tags.
transitive_tag_keys	No	Array of strings	Tag key list that is transparently transmitted along with the temporary security credential in the call chain.

Table 4-389 TagDto

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. Minimum: **1** Maximum: **128**
value	Yes	String	Tag value, which can be an empty string but cannot be null. Minimum: **0** Maximum: **255**

Response Parameters

Status code: 200

Table 4-390 Response body parameters

Parameter	Type	Description
source_identity	String	Identity declared by the initial caller in the call chain. Minimum: **2** Maximum: **64**
assumed_agency	**AssumedAgencyDto** object	Target agency information.
credentials	**CredentialsDto** object	Generated temporary security credential.

Table 4-391 AssumedAgencyDto

Parameter	Type	Description
urn	String	URN of a target agency. Maximum: **1500**
id	String	Unique ID of a target agency, including the agency ID and agency session name. Maximum: **256**

Table 4-392 CredentialsDto

Parameter	Type	Description
access_key_id	String	AK of the temporary security credential. Minimum: **20** Maximum: **20**
expiration	String	Expiration time of the temporary security credential.
secret_access_key	String	SK of the temporary security credential. Minimum: **40** Maximum: **40**
security_token	String	**security_token** of the temporary security credential.

Status code: 400

Table 4-393 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-394 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	Encrypted authentication failure information, which can be decrypted using the STS5 decryption API.

Status code: 404

Table 4-395 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-396 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Obtaining a temporary security credential through agency **Y0yfCQYJGO** of account **27680d67da6b47eb82d00a1a118be145**

```
POST https://{endpoint}/v5/agencies/assume
```



```
{
  "duration_seconds" : 3600,
  "agency_urn" : "iam::27680d67da6b47eb82d00a1a118be145:agency:Y0yfCQYJGO",
  "agency_session_name" : "session1"
}
```

Example Responses

Status code: 200

Successful

```
{
  "assumed_agency" : {
    "urn" : "sts::{account_id}::assumed-agency:{agency_name}/{agency_session_name}",
    "id" : "{agency_id}:{agency_session_name}"
  },
  "credentials" : {
    "access_key_id" : "HSTANO...XBS55JLJ3",
    "secret_access_key" : "EoWCQrr...SCcw4Whkt2aXKWAr",
    "security_token" : "hQpjbi1XXXXXX...XXXXXKbhBbA0TQ==",
    "expiration" : "2022-09-07T03:27:51.158Z"
  }
}
```

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
404	Not found
500	Server error

Error Codes

See **Error Codes**.

4.2.2 Querying the Information of a Caller

4.2.2.1 Obtaining the Identity Information of a Caller

Function

This API is used to obtain the identity information of a caller (such as a user or agency).

Authorization Information

No identity policy-based permission required for calling this API.

URI

GET /v5/caller-identity

Request Parameters

Table 4-397 Request header parameters

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	When an API is called using a temporary security credential, the HTTP request header **X-Security-Token** must be provided. The value is the **security_token** field of the temporary security credential.

Response Parameters

Status code: 200

Table 4-398 Response body parameters

Parameter	Type	Description
account_id	String	Account ID. Maximum: **64**
principal_urn	String	Principal URN. Minimum: **4** Maximum: **1024**
principal_id	String	Principal ID. Minimum: **2** Maximum: **256**

Status code: 500

Table 4-399 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Obtaining the identity information of a caller

```
GET https://{endpoint}/v5/caller-identity
```

Example Responses

Status code: 200

Successful

```
{
  "account_id" : "27680d67da6b47eb82d00a1a118be145",
  "principal_urn" : "iam::27680d67da6b47eb82d00a1a118be145:user:user-name",
  "principal_id" : "user-id"
}
```

Status Codes

Status Code	Description
200	Successful
500	Server error

Error Codes

See **Error Codes**.

4.2.3 Querying the Authentication Result

4.2.3.1 Decoding the Authentication Failure Cause

Function

This API is used to decode the authentication failure cause.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
sts::decodeAuthorizationMessage	Write	-	-	-	-

URI

POST /v5/decode-authorization-message

Request Parameters

Table 4-400 Request header parameters

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	When an API is called using a temporary security credential, the HTTP request header **X-Security-Token** must be provided. The value is the **security_token** field of the temporary security credential.

Table 4-401 Request body parameters

Parameter	Mandatory	Type	Description
encoded_message	Yes	String	Encrypted authentication failure cause. The value is a string and the length is between 1 and 10240. Minimum: **1** Maximum: **10240**

Response Parameters

Status code: 200

Table 4-402 Response body parameters

Parameter	Type	Description
decoded_message	String	Plaintext of the authentication failure cause. Minimum: **1** Maximum: **10240**

Status code: 400

Table 4-403 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-404 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-405 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Decoding the authentication failure cause

```
POST https://{endpoint}/v5/decode-authorization-message

{
  "encoded_message" : "HY0L8G1lOe3rcfgxfKVP+AK+S33eYp/rHQ4l0kJed9...rwaYmLp+pt/ICBwk"
}
```

Example Responses

Status code: 200

Successful

```
{
  "decoded_message" : "{\"context\":{\"user_profile\":...\"failure\":\"implicit deny by identity-based policy\"}"
}
```

Status Codes

Status Code	Description
200	Successful
400	Bad request
403	Forbidden
500	Server error

Error Codes

See **Error Codes**.

4.3 Access Analyzer

4.3.1 Analyzers

4.3.1.1 Retrieving a List of Analyzers

Function

This API is used to retrieve a list of analyzers.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:list	List	analyzer *	-	-	-

URI

GET /v5/analyzers

Table 4-406 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results on a page Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Page marker Minimum: **4** Maximum: **400**
type	No	String	Type of an access analyzer. • **account**: account-level external access analyzer • **organization**: organization-level external access analyzer • **account_unused_access**: account-level unused access analyzer • **organization_unused_access**: organization-level unused access analyzer • **account_privilege_escalation**: account-level privilege escalation access analyzer • **account_iam_best_practice**: account-level IAM best practice analyzer

Request Parameters

None

Response Parameters

Status code: 200

Table 4-407 Response body parameters

Parameter	Type	Description
analyzers	Array of **AnalyzerSummary** objects	Analyzer list details.

Parameter	Type	Description
page_info	**PageInfo** object	Information on the page

Table 4-408 AnalyzerSummary

Parameter	Type	Description
configuration	**AnalyzerConfiguration** object	Analyzer settings.
created_at	String	Time when an analyzer is created
id	String	Unique identifier of an analyzer
last_analyzed_resource	String	Unique identifier of the resource that was recently analyzed.
last_resource_analyzed_at	String	Last time when the access was analyzed.
last_all_analyzed_at	String	Last time when all resources were analyzed.
name	String	Name of an analyzer
organization_id	String	Organization ID.
status	String	Status of an access analyzer. • **active**: The analyzer is activated. • **creating**: The analyzer is being created. • **disabled**: The analyzer is disabled. • **failed**: Failed to create the analyzer.
status_reason	**StatusReason** object	More details about the current status of the analyzer
tags	Array of **Tag** objects	List of custom tags.

Parameter	Type	Description
type	String	Type of an access analyzer. • **account**: account-level external access analyzer • **organization**: organization-level external access analyzer • **account_unused_access**: account-level unused access analyzer • **organization_unused_access**: organization-level unused access analyzer • **account_privilege_escalation**: account-level privilege escalation access analyzer • **account_iam_best_practice**: account-level IAM best practice analyzer
urn	String	Unique resource identifier of an analyzer.

Table 4-409 AnalyzerConfiguration

Parameter	Type	Description
unused_access	**unused_access** object	Settings of an unused access analyzer.

Table 4-410 unused_access

Parameter	Type	Description
unused_access_age	Integer	Preset number of days for generating findings. Minimum: **1** Maximum: **180** Default: **90**
unused_analysis_rule	**UnusedAnalysisRule** object	Unused analysis rule.

Table 4-411 UnusedAnalysisRule

Parameter	Type	Description
exclusions	Array of **UnusedAnalysisRuleCriteria** objects	Exclusion rule.

Table 4-412 UnusedAnalysisRuleCriteria

Parameter	Type	Description
account_ids	Array of strings	Account ID list. Minimum: **1** Maximum: **36** Array Length: **1 - 2000**
resource_tags	Array of **Tag** objects	Resource tag list. Array Length: **1 - 20**

Table 4-413 StatusReason

Parameter	Type	Description
code	String	Reason for the analyzer status. • **delegated_administrator_deregistered**: The delegated administrator is not registered. • **trusted_service_disabled**: The trusted service is disabled. • **internal_error**: There is an internal error. • **organization_deleted**: The organization has been deleted. • **service_linked_agency_creation_failed**: The service-linked agency fails to be created.
details	String	Reason details for the status of the analyzer.

Table 4-414 Tag

Parameter	Type	Description
key	String	Tag key
value	String	String value associated with the tag key.

Table 4-415 PageInfo

Parameter	Type	Description
current_count	Integer	Number of items on the current page
next_marker	String	If present, it indicates that the available output is more than the output contained in the current response. Use this value in the marker request parameter in a subsequent call to the operation to get the next part of the output. You should repeat this operation until the **next_marker** response returns **null**.

Example Requests

Retrieving a list of analyzers

```
GET https://{hostname}/v5/analyzers
```

Example Responses

Status code: 200

OK

```
{
  "analyzers" : [ {
    "created_at" : "2023-09-07T07:26:23.440Z",
    "id" : "{analyzer_id}",
    "last_analyzed_resource" : "iam::{domain_id}:agency:{agency_name}",
    "last_resource_analyzed_at" : "2023-09-07T07:26:23.440Z",
    "name" : "my-analyzer",
    "status" : "active",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
    } ],
    "type" : "account",
    "urn" : "AccessAnalyzer:{region_id}:{domain_id}:analyzer:{analyzer_id}"
  } ],
  "page_info" : {
    "current_count" : 1,
    "next_marker" : null
  }
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.1.2 Creating an Analyzer

Function

This API is used to create an analyzer for your account or organization.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:create	Write	analyzer *	-	-	iam:agencies:createServiceLinkedAgencyV5
		-	• g:RequestTag/<tag-key> • g:TagKeys		

URI

POST /v5/analyzers

Request Parameters

Table 4-416 Request body parameters

Parameter	Mandatory	Type	Description
configuration	No	**AnalyzerConfiguration** object	Analyzer settings.
name	Yes	String	Name of an analyzer

Parameter	Mandatory	Type	Description
tags	No	Array of **Tag** objects	List of custom tags. Array Length: **1 - 20**
type	Yes	String	Type of an access analyzer. • **account**: account-level external access analyzer • **organization**: organization-level external access analyzer • **account_unused_access**: account-level unused access analyzer • **organization_unused_access**: organization-level unused access analyzer • **account_privilege_escalation**: account-level privilege escalation access analyzer • **account_iam_best_practice**: account-level IAM best practice analyzer

Table 4-417 AnalyzerConfiguration

Parameter	Mandatory	Type	Description
unused_access	No	**unused_access** object	Settings of an unused access analyzer.

Table 4-418 unused_access

Parameter	Mandatory	Type	Description
unused_access_age	No	Integer	Preset number of days for generating findings. Minimum: **1** Maximum: **180** Default: **90**
unused_analysis_rule	No	**UnusedAnalysisRule** object	Unused analysis rule.

Table 4-419 UnusedAnalysisRule

Parameter	Mandatory	Type	Description
exclusions	No	Array of **UnusedAnalysisRuleCriteria** objects	Exclusion rule.

Table 4-420 UnusedAnalysisRuleCriteria

Parameter	Mandatory	Type	Description
account_ids	No	Array of strings	Account ID list. Minimum: **1** Maximum: **36** Array Length: **1 - 2000**
resource_tags	No	Array of **Tag** objects	Resource tag list. Array Length: **1 - 20**

Table 4-421 Tag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key
value	Yes	String	String value associated with the tag key.

Response Parameters

Status code: 201

Table 4-422 Response body parameters

Parameter	Type	Description
id	String	Unique identifier of an analyzer
urn	String	Unique resource identifier of an analyzer.

Example Requests

Creating an analyzer for your account or organization


```
POST https://{hostname}/v5/analyzers

{
  "name" : "my-analyzer",
  "tags" : [ {
    "key" : "key-1",
    "value" : "value-1"
  } ],
  "type" : "account"
}
```

Example Responses

Status code: 201

Created

```
{
  "id" : "{analyzer_id}",
  "urn" : "AccessAnalyzer:{region_id}:{domain_id}:analyzer:{analyzer_id}"
}
```

Status Codes

Status Code	Description
201	Created

Error Codes

See **Error Codes**.

4.3.1.3 Listing the Specified Analyzer

Function

This API is used to retrieve information about the specified analyzer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:get	Read	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

GET /v5/analyzers/{analyzer_id}

Table 4-423 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-424 Response body parameters

Parameter	Type	Description
analyzer	**AnalyzerSummary** object	Information about an analyzer

Table 4-425 AnalyzerSummary

Parameter	Type	Description
configuration	**AnalyzerConfiguration** object	Analyzer settings.
created_at	String	Time when an analyzer is created
id	String	Unique identifier of an analyzer
last_analyzed_resource	String	Unique identifier of the resource that was recently analyzed.
last_resource_analyzed_at	String	Last time when the access was analyzed.
last_all_analyzed_at	String	Last time when all resources were analyzed.
name	String	Name of an analyzer
organization_id	String	Organization ID.

Parameter	Type	Description
status	String	Status of an access analyzer. • **active**: The analyzer is activated. • **creating**: The analyzer is being created. • **disabled**: The analyzer is disabled. • **failed**: Failed to create the analyzer.
status_reason	**StatusReason** object	More details about the current status of the analyzer
tags	Array of **Tag** objects	List of custom tags.
type	String	Type of an access analyzer. • **account**: account-level external access analyzer • **organization**: organization-level external access analyzer • **account_unused_access**: account-level unused access analyzer • **organization_unused_access**: organization-level unused access analyzer • **account_privilege_escalation**: account-level privilege escalation access analyzer • **account_iam_best_practice**: account-level IAM best practice analyzer
urn	String	Unique resource identifier of an analyzer.

Table 4-426 AnalyzerConfiguration

Parameter	Type	Description
unused_access	**unused_access** object	Settings of an unused access analyzer.

Table 4-427 unused_access

Parameter	Type	Description
unused_access_age	Integer	Preset number of days for generating findings. Minimum: **1** Maximum: **180** Default: **90**
unused_analysis_rule	**UnusedAnalysisRule** object	Unused analysis rule.

Table 4-428 UnusedAnalysisRule

Parameter	Type	Description
exclusions	Array of **UnusedAnalysisRuleCriteria** objects	Exclusion rule.

Table 4-429 UnusedAnalysisRuleCriteria

Parameter	Type	Description
account_ids	Array of strings	Account ID list. Minimum: **1** Maximum: **36** Array Length: **1 - 2000**
resource_tags	Array of **Tag** objects	Resource tag list. Array Length: **1 - 20**

Table 4-430 StatusReason

Parameter	Type	Description
code	String	Reason for the analyzer status. • **delegated_administrator_deregistered**: The delegated administrator is not registered. • **trusted_service_disabled**: The trusted service is disabled. • **internal_error**: There is an internal error. • **organization_deleted**: The organization has been deleted. • **service_linked_agency_creation_failed**: The service-linked agency fails to be created.
details	String	Reason details for the status of the analyzer.

Table 4-431 Tag

Parameter	Type	Description
key	String	Tag key
value	String	String value associated with the tag key.

Example Requests

Retrieving information about the specified analyzer.

```
GET https://{hostname}/v5/analyzers/{analyzer_id}
```

Example Responses

Status code: 200

OK

```
{
  "analyzer" : {
    "created_at" : "2023-09-07T07:51:10.502Z",
    "id" : "{analyzer_id}",
    "last_analyzed_resource" : "iam::{domain_id}:agency:{agency_name}",
    "last_resource_analyzed_at" : "2023-09-07T07:51:10.502Z",
    "name" : "my-analyzer",
    "status" : "active",
    "tags" : [ {
      "key" : "key-1",
      "value" : "value-1"
```



```
  } ],
  "type" : "account",
  "urn" : "AccessAnalyzer:{region_id}:{domain_id}:analyzer:{analyzer_id}"
 }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.1.4 Deleting the Specified Analyzer

Function

This API is used to delete the specified analyzer. All findings generated by the analyzer will be deleted.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:delete	Write	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

DELETE /v5/analyzers/{analyzer_id}

Table 4-432 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Request Parameters

None

Response Parameters

Status code: 204

Deleted

None

Example Requests

Deleting the specified analyzer

```
DELETE https://{hostname}/v5/analyzers/{analyzer_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	Deleted

Error Codes

See **Error Codes**.

4.3.1.5 Updating the Configuration of an Analyzer

Function

This API is used to update the configuration of an analyzer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:update	Write	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

PUT /v5/analyzers/{analyzer_id}

Table 4-433 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Request Parameters

Table 4-434 Request body parameters

Parameter	Mandatory	Type	Description
configuration	No	**AnalyzerConfiguration** object	Analyzer settings.

Table 4-435 AnalyzerConfiguration

Parameter	Mandatory	Type	Description
unused_access	No	**unused_access** object	Settings of an unused access analyzer.

Table 4-436 unused_access

Parameter	Mandatory	Type	Description
unused_access_age	No	Integer	Preset number of days for generating findings. Minimum: **1** Maximum: **180** Default: **90**
unused_analysis_rule	No	**UnusedAnalysisRule** object	Unused analysis rule.

Table 4-437 UnusedAnalysisRule

Parameter	Mandatory	Type	Description
exclusions	No	Array of **UnusedAnalysisRuleCriteria** objects	Exclusion rule.

Table 4-438 UnusedAnalysisRuleCriteria

Parameter	Mandatory	Type	Description
account_ids	No	Array of strings	Account ID list. Minimum: **1** Maximum: **36** Array Length: **1 - 2000**
resource_tags	No	Array of **Tag** objects	Resource tag list. Array Length: **1 - 20**

Table 4-439 Tag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key
value	Yes	String	String value associated with the tag key.

Response Parameters

Status code: 200

OK

None

Example Requests

Updating the configuration of a specified analyzer

```
PUT https://{hostname}/v5/analyzers/{analyzer_id}

{
  "configuration" : {
    "unused_access" : {
      "unused_access_age" : 30,
      "unused_analysis_rule" : {
        "exclusions" : [ {
          "account_ids" : [ "123", "456" ]
        }, {
          "resource_tags" : [ {
            "key" : "key-1",
            "value" : "value-1"
          }, {
            "key" : "key-2",
            "value" : "value-2"
          } ]
        } ]
      }
    }
  }
}
```

Example Responses

None

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.1.6 Starting Policy Scan for Specified Resources

Function

This API is used to immediately start a scan of the policies applied to the specified resource.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:scan	Write	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

POST /v5/analyzers/{analyzer_id}/scan

Table 4-440 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Request Parameters

Table 4-441 Request body parameters

Parameter	Mandatory	Type	Description
resource_id	No	String	Unique identifier of a resource Minimum: **1** Maximum: **36**
resource_owner_account	Yes	String	ID of the account that owns resources.
resource_project_id	No	String	Identifier of the project that the resource belongs to. Maximum: **36**
resource_urn	Yes	String	Unique identifier of a resource.

Parameter	Mandatory	Type	Description
finding_type	No	String	Finding type. • **external_access**: external access • **privilege_escalation**: privilege escalation • **unused_iam_user_access_key**: unused access key • **unused_iam_user_password**: unused password • **unused_permission**: unused permission • **unused_iam_agency**: unused agency • **iam_bp_root_user_has_access_key**: an AK/SK pair is bound to the root user • **iam_bp_access_api_with_password**: APIs access using passwords • **iam_bp_login_protection_disabled**: login protection disabled • **iam_bp_mfa_unconfigured**: MFA not added • **iam_bp_assign_high_risk_sys_policy_or_role_to_user**: high-risk system-defined policies or roles attached to users • **iam_bp_attach_high_risk_sys_identity_policy_to_user**: high-risk system-defined identity policies attached to users • **iam_bp_assign_high_risk_sys_policy_or_role_to_agency**: high-risk system-defined policies or roles attached to agencies • **iam_bp_attach_high_risk_sys_identity_policy_to_agency**: high-risk system-defined identity policies attached to agencies

Response Parameters

Status code: 200

OK

None

Example Requests

Immediately starting a scan of the policies applied to the specified resource

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/scan

{
  "resource_owner_account" : "{analyzer_id}",
  "resource_urn" : "iam::{domain_id}:agency:{agency_name}",
  "resource_id" : "{agency_id}"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.2 Archive Rules

4.3.2.1 Creating an Archive Rule for the Specified Analyzer

Function

This API is used to create an archive rule for the specified analyzer. The archive rule will automatically archive new findings that meet the criteria you define when you create the rule.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:archiveRule:create	Write	archiveRule *	-	-	-

URI

POST /v5/analyzers/{analyzer_id}/archive-rules

Table 4-442 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Request Parameters

Table 4-443 Request body parameters

Parameter	Mandatory	Type	Description
filters	Yes	Array of **FindingFilter** objects	A filter to match the returned findings. Array Length: **1 - 10**
name	Yes	String	Name of the archive rule.

Table 4-444 FindingFilter

Parameter	Mandatory	Type	Description
criterion	Yes	**Criterion** object	Criteria in the filter. Only one operator is allowed.

Parameter	Mandatory	Type	Description
key	Yes	String	Filter key. • **resource**: resource URN • **resource_type**: resource type • **resource_owner_account**: resource owner account • **is_public**: public access permission • **id**: finding ID • **status**: finding type • **principal_type** • **principal_identifier** • **change_type**: finding status change • **existing_finding_id**: ID of an existing finding • **existing_finding_status**: status of an existing finding • **condition.g:PrincipalUrn**: principal URN • **condition.g:PrincipalId**: principal ID • **condition.g:PrincipalAccount**: principal account • **condition.g:PrincipalOrgId**: principal organization ID • **condition.g:PrincipalOrgPath**: principal organization path • **condition.g:PrincipalOrgManagementAccountId**: principal organization management account ID • **condition.g:SourceIp**: source IP address • **condition.g:SourceVpc**: source VPC • **condition.g: SourceVpce**: source VPC endpoint • **finding_type**: finding type

Table 4-445 Criterion

Parameter	Mandatory	Type	Description
contains	No	Array of strings	Matching the "contains" operator in the filter Array Length: **1 - 20**
eq	No	Array of strings	Matching the "eq" operator in the filter Array Length: **1 - 20**
exists	No	Boolean	Matching the "exists" operator in the filter
neq	No	Array of strings	Matching the "neq" operator in the filter Array Length: **1 - 20**

Response Parameters

Status code: 201

Table 4-446 Response body parameters

Parameter	Type	Description
id	String	Unique identifier of an archive rule
urn	String	Unique resource identifier of an archive rule.

Example Requests

Creating an archive rule for a specified analyzer. The archive rule automatically archives new findings that meet the criteria you define when you create the rule.

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/archive-rules

{
  "filters" : [ {
    "criterion" : {
      "eq" : [ "iam:agency" ]
    },
    "key" : "resource_type"
  } ],
  "name" : "my-archive-rules"
}
```

Example Responses

Status code: 201

Created


```
{
  "id" : "{archive_rule_id}",
  "urn" : "AccessAnalyzer:{region_id}:{domain_id}:archiveRule:{analyzer_id}/{archive_rule_id}"
}
```

Status Codes

Status Code	Description
201	Created

Error Codes

See **Error Codes**.

4.3.2.2 Retrieving a List of Archive Rules Created for the Specified Analyzer

Function

This API is used to retrieve a list of archive rules created for the specified analyzer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:archiveRule:list	List	archiveRule *	-	-	-

URI

GET /v5/analyzers/{analyzer_id}/archive-rules

Table 4-447 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Table 4-448 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results on a page Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Page marker Minimum: **4** Maximum: **400**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-449 Response body parameters

Parameter	Type	Description
archive_rules	Array of **ArchiveRuleSummary** objects	List of archive rules created for the specified analyzer.
page_info	**PageInfo** object	Information on the page

Table 4-450 ArchiveRuleSummary

Parameter	Type	Description
created_at	String	Time when an archive rule was created.
filters	Array of **FindingFilter** objects	A filter to match the returned findings.
id	String	Unique identifier of an archive rule
name	String	Name of the archive rule.
updated_at	String	Time when the archive rule was last updated

Parameter	Type	Description
urn	String	Unique resource identifier of an archive rule.

Table 4-451 FindingFilter

Parameter	Type	Description
criterion	**Criterion** object	Criteria in the filter. Only one operator is allowed.

Parameter	Type	Description
key	String	Filter key. • **resource**: resource URN • **resource_type**: resource type • **resource_owner_account**: resource owner account • **is_public**: public access permission • **id**: finding ID • **status**: finding type • **principal_type** • **principal_identifier** • **change_type**: finding status change • **existing_finding_id**: ID of an existing finding • **existing_finding_status**: status of an existing finding • **condition.g:PrincipalUrn**: principal URN • **condition.g:PrincipalId**: principal ID • **condition.g:PrincipalAccount**: principal account • **condition.g:PrincipalOrgId**: principal organization ID • **condition.g:PrincipalOrgPath**: principal organization path • **condition.g:PrincipalOrgManagementAccountId**: principal organization management account ID • **condition.g:SourceIp**: source IP address • **condition.g:SourceVpc**: source VPC • **condition.g: SourceVpce**: source VPC endpoint • **finding_type**: finding type

Table 4-452 Criterion

Parameter	Type	Description
contains	Array of strings	Matching the "contains" operator in the filter Array Length: **1 - 20**
eq	Array of strings	Matching the "eq" operator in the filter Array Length: **1 - 20**
exists	Boolean	Matching the "exists" operator in the filter
neq	Array of strings	Matching the "neq" operator in the filter Array Length: **1 - 20**

Table 4-453 PageInfo

Parameter	Type	Description
current_count	Integer	Number of items on the current page
next_marker	String	If present, it indicates that the available output is more than the output contained in the current response. Use this value in the marker request parameter in a subsequent call to the operation to get the next part of the output. You should repeat this operation until the **next_marker** response returns **null**.

Example Requests

Retrieving a list of archive rules created for the specified analyzer

```
GET https://{hostname}/v5/analyzers/{analyzer_id}/archive-rules
```

Example Responses

Status code: 200

OK

```
{
  "archive_rules" : [ {
    "created_at" : "2023-09-07T08:35:41.997Z",
    "filters" : [ {
      "criterion" : {
        "eq" : [ "iam:agency" ]
      },
```



```
    "key" : "resource_type"
  } ],
  "id" : "{archive_rule_id}",
  "name" : "my-archive-rules",
  "updated_at" : "2023-09-07T08:35:41.997Z",
  "urn" : "AccessAnalyzer:{region_id}:{domain_id}:archiveRule:{analyzer_id}/{archive_rule_id}"
 } ],
 "page_info" : {
  "current_count" : 1,
  "next_marker" : null
 }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.2.3 Retrieving Information About an Archive Rule

Function

This API is used to retrieve information about an archive rule.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:archiveRule:get	Read	archiveRule *	-	-	-

URI

GET /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}

Table 4-454 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**
archive_rule_id	Yes	String	Unique identifier of an archive rule Minimum: **1** Maximum: **36**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-455 Response body parameters

Parameter	Type	Description
archive_rule	**ArchiveRuleSummary** object	Archive rule created by an analyzer.

Table 4-456 ArchiveRuleSummary

Parameter	Type	Description
created_at	String	Time when an archive rule was created.
filters	Array of **FindingFilter** objects	A filter to match the returned findings.
id	String	Unique identifier of an archive rule
name	String	Name of the archive rule.
updated_at	String	Time when the archive rule was last updated
urn	String	Unique resource identifier of an archive rule.

Table 4-457 FindingFilter

Parameter	Type	Description
criterion	**Criterion** object	Criteria in the filter. Only one operator is allowed.
key	String	Filter key. • **resource**: resource URN • **resource_type**: resource type • **resource_owner_account**: resource owner account • **is_public**: public access permission • **id**: finding ID • **status**: finding type • **principal_type** • **principal_identifier** • **change_type**: finding status change • **existing_finding_id**: ID of an existing finding • **existing_finding_status**: status of an existing finding • **condition.g:PrincipalUrn**: principal URN • **condition.g:PrincipalId**: principal ID • **condition.g:PrincipalAccount**: principal account • **condition.g:PrincipalOrgId**: principal organization ID • **condition.g:PrincipalOrgPath**: principal organization path • **condition.g:PrincipalOrgManagementAccountId**: principal organization management account ID • **condition.g:SourceIp**: source IP address • **condition.g:SourceVpc**: source VPC • **condition.g: SourceVpce**: source VPC endpoint • **finding_type**: finding type

Table 4-458 Criterion

Parameter	Type	Description
contains	Array of strings	Matching the "contains" operator in the filter Array Length: **1 - 20**
eq	Array of strings	Matching the "eq" operator in the filter Array Length: **1 - 20**
exists	Boolean	Matching the "exists" operator in the filter
neq	Array of strings	Matching the "neq" operator in the filter Array Length: **1 - 20**

Example Requests

Retrieving information about an archive rule

```
GET https://{hostname}/v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}
```

Example Responses

Status code: 200

OK

```
{
  "archive_rule" : {
    "created_at" : "2023-09-07T08:35:41.997Z",
    "filters" : [ {
      "criterion" : {
        "eq" : [ "iam:agency" ]
      },
      "key" : "resource_type"
    } ],
    "id" : "{archive_rule_id}",
    "name" : "my-archive-rules",
    "updated_at" : "2023-09-07T08:35:41.997Z",
    "urn" : "AccessAnalyzer:{region_id}:{domain_id}:archiveRule:{analyzer_id}/{archive_rule_id}"
  }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.2.4 Deleting the Specified Archive Rule

Function

This API is used to delete the specified archive rule.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:archiveRule:delete	Write	archiveRule *	-	-	-

URI

DELETE /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}

Table 4-459 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**
archive_rule_id	Yes	String	Unique identifier of an archive rule Minimum: **1** Maximum: **36**

Request Parameters

None

Response Parameters

Status code: 204

Deleted

None

Example Requests

Deleting the specified archive rule

```
DELETE https://{hostname}/v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	Deleted

Error Codes

See **Error Codes**.

4.3.2.5 Updating the Criteria and Values of the Specified Archive Rule

Function

This API is used to update the criteria and values of the specified archive rule.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:archiveRule:update	Write	archiveRule *	-	-	-

URI

PUT /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}

Table 4-460 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**
archive_rule_id	Yes	String	Unique identifier of an archive rule Minimum: **1** Maximum: **36**

Request Parameters

Table 4-461 Request body parameters

Parameter	Mandatory	Type	Description
filters	Yes	Array of **FindingFilter** objects	A filter to match the returned findings. Array Length: **1 - 10**

Table 4-462 FindingFilter

Parameter	Mandatory	Type	Description
criterion	Yes	**Criterion** object	Criteria in the filter. Only one operator is allowed.

Parameter	Mandatory	Type	Description
key	Yes	String	Filter key. • **resource**: resource URN • **resource_type**: resource type • **resource_owner_account**: resource owner account • **is_public**: public access permission • **id**: finding ID • **status**: finding type • **principal_type** • **principal_identifier** • **change_type**: finding status change • **existing_finding_id**: ID of an existing finding • **existing_finding_status**: status of an existing finding • **condition.g:PrincipalUrn**: principal URN • **condition.g:PrincipalId**: principal ID • **condition.g:PrincipalAccount**: principal account • **condition.g:PrincipalOrgId**: principal organization ID • **condition.g:PrincipalOrgPath**: principal organization path • **condition.g:PrincipalOrgManagementAccountId**: principal organization management account ID • **condition.g:SourceIp**: source IP address • **condition.g:SourceVpc**: source VPC • **condition.g: SourceVpce**: source VPC endpoint • **finding_type**: finding type

Table 4-463 Criterion

Parameter	Mandatory	Type	Description
contains	No	Array of strings	Matching the "contains" operator in the filter Array Length: **1 - 20**
eq	No	Array of strings	Matching the "eq" operator in the filter Array Length: **1 - 20**
exists	No	Boolean	Matching the "exists" operator in the filter
neq	No	Array of strings	Matching the "neq" operator in the filter Array Length: **1 - 20**

Response Parameters

Status code: 200

OK

None

Example Requests

Updating the criteria and values of the specified archive rule

```
PUT https://{hostname}/v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}

{
  "filters" : [ {
    "criterion" : {
      "eq" : [ "iam:agency" ]
    },
    "key" : "resource_type"
  }, {
    "criterion" : {
      "eq" : [ "obs:bucket" ]
    },
    "key" : "resource_type"
  } ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.2.6 Applying Archiving Rules

Function

This API is used to apply archiving rules retroactively to archive existing findings that meet the archive rule criteria.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:archiveRule:apply	Write	archiveRule *	-	-	-

URI

POST /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}/apply

Table 4-464 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Parameter	Mandatory	Type	Description
archive_rule_id	Yes	String	Unique identifier of an archive rule Minimum: **1** Maximum: **36**

Request Parameters

None

Response Parameters

Status code: 200

OK

None

Example Requests

Applying archiving rules retroactively to archive existing findings that meet the archive rule criteria

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}/apply
```

Example Responses

None

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.3 Findings

4.3.3.1 Retrieving a List of Findings Generated by the Specified Analyzer

Function

This API is used to retrieve a list of findings generated by the specified analyzer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:listFindings	List	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

POST /v5/analyzers/{analyzer_id}/findings

Table 4-465 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Request Parameters

Table 4-466 Request body parameters

Parameter	Mandatory	Type	Description
filters	No	Array of **FindingFilter** objects	A filter to match the returned findings. Array Length: **1 - 20**
limit	No	Integer	Maximum number of results on a page
marker	No	String	Page marker

Table 4-467 FindingFilter

Parameter	Mandatory	Type	Description
criterion	Yes	Criterion object	Criteria in the filter. Only one operator is allowed.
key	Yes	String	Filter key. • **resource**: resource URN • **resource_type**: resource type • **resource_owner_account**: resource owner account • **is_public**: public access permission • **id**: finding ID • **status**: finding type • **principal_type** • **principal_identifier** • **change_type**: finding status change • **existing_finding_id**: ID of an existing finding • **existing_finding_status**: status of an existing finding • **condition.g:PrincipalUrn**: principal URN • **condition.g:PrincipalId**: principal ID • **condition.g:PrincipalAccount**: principal account • **condition.g:PrincipalOrgId**: principal organization ID • **condition.g:PrincipalOrgPath**: principal organization path • **condition.g:PrincipalOrgManagementAccountId**: principal organization management account ID • **condition.g:SourceIp**: source IP address • **condition.g:SourceVpc**: source VPC • **condition.g: SourceVpce**: source VPC endpoint • **finding_type**: finding type

Table 4-468 Criterion

Parameter	Mandatory	Type	Description
contains	No	Array of strings	Matching the "contains" operator in the filter Array Length: **1 - 20**
eq	No	Array of strings	Matching the "eq" operator in the filter Array Length: **1 - 20**
exists	No	Boolean	Matching the "exists" operator in the filter
neq	No	Array of strings	Matching the "neq" operator in the filter Array Length: **1 - 20**

Response Parameters

Status code: 200

Table 4-469 Response body parameters

Parameter	Type	Description
findings	Array of **FindingSummary** objects	List of findings.
page_info	**PageInfo** object	Information on the page

Table 4-470 FindingSummary

Parameter	Type	Description
action	Array of strings	Action that can be used by external principals.
analyzed_at	String	Time when resources were analyzed.
condition	Array of **FindingCondition** objects	Condition that generates findings in the policy statement.
created_at	String	Time when the findings were generated.

Parameter	Type	Description
finding_type	String	Finding type. • **external_access**: external access • **privilege_escalation**: privilege escalation • **unused_iam_user_access_key**: unused access key • **unused_iam_user_password**: unused password • **unused_permission**: unused permission • **unused_iam_agency**: unused agency • **iam_bp_root_user_has_access_key**: an AK/SK pair is bound to the root user • **iam_bp_access_api_with_password**: APIs access using passwords • **iam_bp_login_protection_disabled**: login protection disabled • **iam_bp_mfa_unconfigured**: MFA not added • **iam_bp_assign_high_risk_sys_policy_or_role_to_user**: high-risk system-defined policies or roles attached to users • **iam_bp_attach_high_risk_sys_identity_policy_to_user**: high-risk system-defined identity policies attached to users • **iam_bp_assign_high_risk_sys_policy_or_role_to_agency**: high-risk system-defined policies or roles attached to agencies • **iam_bp_attach_high_risk_sys_identity_policy_to_agency**: high-risk system-defined identity policies attached to agencies
id	String	Unique identifier of a finding.
is_public	Boolean	Whether the policy that generates findings allows public access to resources.
principal	**FindingPrincipal** object	An external principal that accesses resources in a zone of trust.

Parameter	Type	Description
resource	String	Unique identifier of a resource.
resource_id	String	Unique identifier of a resource. Minimum: **1** Maximum: **36**
resource_owner_account	String	ID of the account that owns resources.
resource_project_id	String	Identifier of the project that the resource belongs to. Maximum: **36**
resource_type	String	Resource type. • **iam:agency**: IAM agency • **iam:user**: IAM user • **kms:cmk**: DEW shared key • **obs:bucket**: OBS bucket • **swr:repo**: SWR image repository • **cbr:backup**: CBR backup • **ims:image**: IMS image
sources	Array of strings	Source of findings, indicating how to grant access that generates the findings.
status	String	Finding status. • **active** • **archived** • **resolved**
updated_at	String	Time when the findings are updated.

Table 4-471 FindingCondition

Parameter	Type	Description
key	String	Identifier or name of a condition key.
value	String	Value of the condition key.

Table 4-472 FindingPrincipal

Parameter	Type	Description
identifier	String	Identifier of a principal.

Parameter	Type	Description
type	String	Type of a principal. • **all_principal**: all principals • **account** • **all_user_in_account**: all users in an account • **all_agency_in_account**: all agencies in an account • **all_identity_provider_in_account**: all identity providers in an account • **specific_user**: specific user • **specific_agency**: specific agency • **specific_group**: specific user group • **specific_identity_provider**: specific identity provider

Table 4-473 PageInfo

Parameter	Type	Description
current_count	Integer	Number of items on the current page
next_marker	String	If present, it indicates that the available output is more than the output contained in the current response. Use this value in the marker request parameter in a subsequent call to the operation to get the next part of the output. You should repeat this operation until the **next_marker** response returns **null**.

Example Requests

Retrieving a list of findings generated by the specified analyzer

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/findings

{
  "filters" : [ {
    "criterion" : {
      "eq" : [ "iam:agency" ]
    },
    "key" : "resource_type"
  } ],
  "limit" : 100,
  "marker" : "{marker_string}"
}
```


Example Responses

Status code: 200

OK


```
{
  "findings" : [ {
    "action" : [ "sts:agencies:assume" ],
    "analyzed_at" : "2023-09-07T08:04:41.698Z",
    "condition" : [ {
      "key" : "g:PrincipalOrgId",
      "value" : "org_id"
    } ],
    "created_at" : "2023-09-07T08:04:41.698Z",
    "id" : "{finding_id}",
    "is_public" : false,
    "principal" : {
      "identifier" : "{domain_id}",
      "type" : "account"
    },
    "resource" : "iam::{domain_id}:agency:{agency_name}",
    "resource_owner_account" : "{domain_id}",
    "resource_id" : "{agency_id}",
    "resource_type" : "iam:agency",
    "status" : "active",
    "updated_at" : "2023-09-07T08:04:41.698Z"
  } ],
  "page_info" : {
    "current_count" : 1,
    "next_marker" : null
  }
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.3.2 Updating the Status of the Specified Findings

Function

This API is used to update the status of a specified finding.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:updateFindings	Write	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

PUT /v5/analyzers/{analyzer_id}/findings

Table 4-474 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Request Parameters

Table 4-475 Request body parameters

Parameter	Mandatory	Type	Description
ids	No	Array of strings	Unique identifier array of findings to be updated. Array Length: **1 - 50**
resource_urn	No	String	Unique identifier of a resource.
status	Yes	String	Status of the findings to be updated. • **active** • **archived**

Response Parameters

Status code: 200

OK

None

Example Requests

Updating the status of the specified findings

```
PUT https://{hostname}/v5/analyzers/{analyzer_id}/findings

{
  "ids" : [ "{finding_id}" ],
  "resource_urn" : "iam::{domain_id}:agency:{agency_name}",
  "status" : "active"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.3.3 Retrieving Information About the Specified Finding

Function

This API is used to retrieve information about the specified finding.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:getFinding	Read	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

GET /v5/analyzers/{analyzer_id}/findings/{finding_id}

Table 4-476 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**
finding_id	Yes	String	Unique identifier of a finding. Minimum: **1** Maximum: **36**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-477 Response body parameters

Parameter	Type	Description
finding	**Finding** object	Findings.

Table 4-478 Finding

Parameter	Type	Description
action	Array of strings	Action that can be used by external principals.
analyzed_at	String	Time when a resource is analyzed
condition	Array of **FindingCondition** objects	Condition that generates findings in the policy statement.
created_at	String	Time when the findings were generated.
finding_details	Array of **FindingDetails** objects	Finding details.

Parameter	Type	Description
finding_type	String	Finding type. • **external_access**: external access • **privilege_escalation**: privilege escalation • **unused_iam_user_access_key**: unused access key • **unused_iam_user_password**: unused password • **unused_permission**: unused permission • **unused_iam_agency**: unused agency • **iam_bp_root_user_has_access_key**: an AK/SK pair is bound to the root user • **iam_bp_access_api_with_password**: APIs access using passwords • **iam_bp_login_protection_disabled**: login protection disabled • **iam_bp_mfa_unconfigured**: MFA not added • **iam_bp_assign_high_risk_sys_policy_or_role_to_user**: high-risk system-defined policies or roles attached to users • **iam_bp_attach_high_risk_sys_identity_policy_to_user**: high-risk system-defined identity policies attached to users • **iam_bp_assign_high_risk_sys_policy_or_role_to_agency**: high-risk system-defined policies or roles attached to agencies • **iam_bp_attach_high_risk_sys_identity_policy_to_agency**: high-risk system-defined identity policies attached to agencies
id	String	Unique identifier of a finding.
is_public	Boolean	Whether the policy that generates findings allows public access to resources.
principal	**FindingPrincipal** object	An external principal that accesses resources in a zone of trust.

Parameter	Type	Description
resource	String	Unique identifier of a resource.
resource_id	String	Unique identifier of a resource Minimum: **1** Maximum: **36**
resource_owner_account	String	ID of the account that owns resources.
resource_project_id	String	Identifier of the project that the resource belongs to. Maximum: **36**
resource_type	String	Resource type. • **iam:agency**: IAM agency • **iam:user**: IAM user • **kms:cmk**: DEW shared key • **obs:bucket**: OBS bucket • **swr:repo**: SWR image repository • **cbr:backup**: CBR backup • **ims:image**: IMS image
sources	Array of strings	Source of findings, indicating how to grant access that generates the findings.
status	String	Finding status. • **active** • **archived** • **resolved**
updated_at	String	Time when the findings were updated.

Table 4-479 FindingDetails

Parameter	Type	Description
external_access_details	**ExternalAccessDetails** object	External access findings.
privilege_escalation_details	**PrivilegeEscalationDetails** object	Finding details for privilege escalation access.
unused_iam_user_access_key_details	**UnusedIamUserAccessKeyDetails** object	Finding details for unused keys.

Parameter	Type	Description
unused_iam_user_password_details	**UnusedIamUserPasswordDetails** object	Finding details for unused user passwords.
unused_permission_details	**UnusedPermissionDetails** object	Finding details for unused permissions.
unused_iam_agency_details	**UnusedIamAgencyDetails** object	Finding details for unused agencies.
iam_bp_root_user_has_access_key_details	**IamBpRootUserHasAccessKeyDetails** object	Finding details for root users who have access keys.
iam_bp_access_api_with_password_details	**IamBpAccessApiWithPasswordDetails** object	Finding details for API access with passwords.
iam_bp_login_protection_disabled_details	**IamBpLoginProtectionDisabledDetails** object	Finding details for disabled login protection.
iam_bp_mfa_unconfigured_details	**IamBpMfaUnconfiguredDetails** object	Finding details for unbound MFA.
iam_bp_assign_high_risk_sys_policy_or_role_to_user_details	**IamBpAssignHighRiskSysPolicyOrRoleToUserDetails** object	Finding details for attaching high-risk system permissions or roles to IAM users.
iam_bp_attach_high_risk_sys_identity_policy_to_user_details	**IamBpAttachHighRiskSysIdentityPolicyToUserDetails** object	Finding details for attaching high-risk system identity policies to IAM users.
iam_bp_assign_high_risk_sys_policy_or_role_to_agency_details	**IamBpAssignHighRiskSysPolicyOrRoleToAgencyDetails** object	Finding details for attaching high-risk system policies or roles to IAM agencies.
iam_bp_attach_high_risk_sys_identity_policy_to_agency_details	**IamBpAttachHighRiskSysIdentityPolicyToAgencyDetails** object	Finding details for attaching high-risk system identity policies to IAM agencies.

Table 4-480 ExternalAccessDetails

Parameter	Type	Description
action	Array of strings	Action that can be used by external principals.

Parameter	Type	Description
condition	Array of **FindingCondition** objects	Condition that generates findings in the policy statement.
is_public	Boolean	Whether the policy that generates findings allows public access to resources.
principal	**FindingPrincipal** object	An external principal that accesses resources in a zone of trust.
sources	Array of strings	Source of findings, indicating how to grant access that generates the findings.

Table 4-481 FindingCondition

Parameter	Type	Description
key	String	Identifier or name of a condition key.
value	String	Value of the condition key.

Table 4-482 PrivilegeEscalationDetails

Parameter	Type	Description
actions	Array of strings	Specified set of operations to be analyzed.
resource	String	Unique identifier of a resource.
principal	**FindingPrincipal** object	Principal that accesses resources in a zone of trust.
active_action	String	Operations that can be triggered through privilege escalation access paths.
path	Array of **PrivilegeEscalationStep** objects	Step of the privilege escalation access path.

Table 4-483 PrivilegeEscalationStep

Parameter	Type	Description
principal	**FindingPrincipal** object	Principal that accesses resources in a zone of trust.
resources	Array of strings	Resources involved in this step.
action	String	Operations involved in this step.

Table 4-484 UnusedIamUserAccessKeyDetails

Parameter	Type	Description
access_key_id	String	Unique ID of a user access key.
last_accessed	String	Last access time of a user access key.

Table 4-485 UnusedIamUserPasswordDetails

Parameter	Type	Description
last_accessed	String	Last access time of a user password.

Table 4-486 UnusedPermissionDetails

Parameter	Type	Description
service	String	Name of the cloud service that the permission belongs to.
last_accessed	String	Last access time of the cloud service.
actions	Array of **UnusedAction** objects	Unused actions.

Table 4-487 UnusedAction

Parameter	Type	Description
action	String	Authorization item name.
last_accessed	String	Last access time of the authorization item.

Table 4-488 UnusedIamAgencyDetails

Parameter	Type	Description
last_accessed	String	Last access time of the agency.

Table 4-489 IamBpRootUserHasAccessKeyDetails

Parameter	Type	Description
access_key_id	String	Unique ID of a user access key. Minimum: **1** Maximum: **40**
last_accessed	String	Last access time of a user access key.
created_at	String	Time when the user access key is created.

Table 4-490 IamBpAccessApiWithPasswordDetails

Parameter	Type	Description
user_id	String	Unique ID of the user. Minimum: **1** Maximum: **36**
last_access_api_with_pwd_at	String	Last time when a user accessed APIs with a password.
user_created_at	String	Time when the user was created.

Table 4-491 IamBpLoginProtectionDisabledDetails

Parameter	Type	Description
user_id	String	Unique ID of the user. Minimum: **1** Maximum: **36**
user_created_at	String	Time when the user was created.

Table 4-492 IamBpMfaUnconfiguredDetails

Parameter	Type	Description
user_id	String	Unique ID of the user. Minimum: **1** Maximum: **36**
user_created_at	String	Time when the user was created.

Table 4-493 IamBpAssignHighRiskSysPolicyOrRoleToUserDetails

Parameter	Type	Description
user_id	String	Unique ID of the user. Minimum: **1** Maximum: **36**
permission_name	String	Permission name.

Table 4-494 IamBpAttachHighRiskSysIdentityPolicyToUserDetails

Parameter	Type	Description
user_id	String	Unique ID of the user. Minimum: **1** Maximum: **36**
policy_name	String	Policy name.

Table 4-495 IamBpAssignHighRiskSysPolicyOrRoleToAgencyDetails

Parameter	Type	Description
agency_id	String	Unique ID of the agency. Minimum: **1** Maximum: **36**
permission_name	String	Permission name.

Table 4-496 IamBpAttachHighRiskSysIdentityPolicyToAgencyDetails

Parameter	Type	Description
agency_id	String	Unique ID of the agency. Minimum: **1** Maximum: **36**
policy_name	String	Policy name.

Table 4-497 FindingPrincipal

Parameter	Type	Description
identifier	String	Identifier of a principal.
type	String	Type of a principal. • **all_principal**: all principals • **account** • **all_user_in_account**: all users in an account • **all_agency_in_account**: all agencies in an account • **all_identity_provider_in_account**: all identity providers in an account • **specific_user**: specific user • **specific_agency**: specific agency • **specific_group**: specific user group • **specific_identity_provider**: specific identity provider

Example Requests

Retrieving information about the specified finding

```
GET https://{hostname}/v5/analyzers/{analyzer_id}/findings/{finding_id}
```

Example Responses

Status code: 200

OK

```
{
  "finding" : {
    "action" : [ "obs:bucket:listBucket" ],
    "analyzed_at" : "2023-09-07T08:04:41.698Z",
    "condition" : [ {
      "key" : "g:PrincipalOrgId",
      "value" : "org_id"
    } ],
```

```
    "created_at" : "2023-09-07T08:04:41.698Z",
    "id" : "{finding_id}",
    "is_public" : false,
    "principal" : {
      "identifier" : "{domain_id}",
      "type" : "account"
    },
    "resource" : "obs:{region_id}::bucket:{bucket_name}",
    "resource_owner_account" : "{domain_id}",
    "resource_type" : "obs:bucket",
    "sources" : [ "bucket_policy" ],
    "status" : "active",
    "updated_at" : "2023-09-07T08:04:41.698Z"
  }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.4 Access Preview

4.3.4.1 Creating an Access Preview

Function

This API is used to create an access preview.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:createPreview	Write	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

POST /v5/analyzers/{analyzer_id}/access-previews

Table 4-498 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Request Parameters

Table 4-499 Request body parameters

Parameter	Mandatory	Type	Description
configurations	Yes	**Configuration** object	Preview access settings.
resource_urn	Yes	String	Unique identifier of a resource.

Table 4-500 Configuration

Parameter	Mandatory	Type	Description
iam_agency	No	**IAMAgency** object	IAM trust agency.
obs_bucket	No	**OBSBucket** object	OBS bucket.
kms_cmk	No	**KMSCmk** object	KMS key.

Table 4-501 IAMAgency

Parameter	Mandatory	Type	Description
trust_policy	Yes	String	JSON policy document.

Table 4-502 OBSBucket

Parameter	Mandatory	Type	Description
bucket_acl	No	String	String format of the bucket ACL XML file.
bucket_policy	No	String	JSON policy document.

Table 4-503 KMSCmk

Parameter	Mandatory	Type	Description
grants	Yes	String	Used to authorize encryption keys.

Response Parameters

Status code: 201

Table 4-504 Response body parameters

Parameter	Type	Description
access_preview_id	String	Unique identifier of an access preview.

Example Requests

Creating an access preview

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/access-previews

{
  "resource_urn" : "iam::{domain_id}:agency:{agency_name}",
  "configurations" : {
    "iam_agency" : {
      "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Condition\":{\"StringMatch\":{\"g:PrincipalOrgId\":
[\"org_id\"]}},\"Action\":[\"sts:agencies:assume\",\"sts::tagSession\",\"sts::setSourceIdentity\"],\"Effect
\":\"Allow\",\"Principal\":{\"IAM\":[\"dd...\"]}}]}"
    }
  }
}
```

Example Responses

Status code: 201

Created

```
{
  "access_preview_id" : "{access_preview_id}"
}
```


Status Codes

Status Code	Description
201	Created

Error Codes

See **Error Codes**.

4.3.4.2 Obtaining All Access Previews

Function

This API is used to obtain all access previews.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:listPreviews	List	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

GET /v5/analyzers/{analyzer_id}/access-previews

Table 4-505 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Table 4-506 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results on a page Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Page marker Minimum: **4** Maximum: **400**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-507 Response body parameters

Parameter	Type	Description
access_previews	Array of **AccessPreviewSummary** objects	Access preview list.
page_info	**PageInfo** object	Information on the page

Table 4-508 AccessPreviewSummary

Parameter	Type	Description
access_preview_id	String	Unique identifier of an access preview.
analyzer_id	String	Unique identifier of an analyzer
created_at	String	Time when the access preview was created.
status	String	Status of an access preview. • **creating**: The preview is being created. • **completed**: The preview is created. • **failed**: Failed to create the preview.

Parameter	Type	Description
status_reason	**PreviewStatusReason** object	More details about the status of an access preview.

Table 4-509 PreviewStatusReason

Parameter	Type	Description
code	String	Reason for the status of an access preview.

Table 4-510 PageInfo

Parameter	Type	Description
current_count	Integer	Number of items on the current page
next_marker	String	If present, it indicates that the available output is more than the output contained in the current response. Use this value in the marker request parameter in a subsequent call to the operation to get the next part of the output. You should repeat this operation until the **next_marker** response returns **null**.

Example Requests

Obtaining all access previews

```
GET https://{hostname}/v5/analyzers/{analyzer_id}/access-previews
```

Example Responses

Status code: 200

OK

```
{
  "access_previews" : [ {
    "analyzer_id" : "{analyzer_id}",
    "created_at" : "2023-09-07T08:35:41.997Z",
    "access_preview_id" : "{access_preview_id}",
    "status" : "completed"
  } ],
  "page_info" : {
    "current_count" : 1,
    "next_marker" : null
  }
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.4.3 Obtaining Access Preview Details

Function

This API is used to obtain access preview details.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:getPreview	Read	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

GET /v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}

Table 4-511 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**
access_preview_id	Yes	String	Unique identifier of an access preview. Minimum: **1** Maximum: **36**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-512 Response body parameters

Parameter	Type	Description
access_preview	**AccessPreview** object	An access preview.

Table 4-513 AccessPreview

Parameter	Type	Description
access_preview_id	String	Unique identifier of an access preview.
analyzer_id	String	Unique identifier of an analyzer
configurations	**Configuration** object	Preview access settings.
created_at	String	Time when the access preview is created.
status	String	Status of an access preview. • **creating**: The preview is being created. • **completed**: The preview is created. • **failed**: Failed to create the preview.
status_reason	**PreviewStatusReason** object	More details about the status of an access preview.

Table 4-514 Configuration

Parameter	Type	Description
iam_agency	**IAMAgency** object	IAM trust agency.
obs_bucket	**OBSBucket** object	OBS bucket.
kms_cmk	**KMSCmk** object	KMS key.

Table 4-515 IAMAgency

Parameter	Type	Description
trust_policy	String	JSON policy document.

Table 4-516 OBSBucket

Parameter	Type	Description
bucket_acl	String	String format of the bucket ACL XML file.
bucket_policy	String	JSON policy document.

Table 4-517 KMSCmk

Parameter	Type	Description
grants	String	Used to authorize encryption keys.

Table 4-518 PreviewStatusReason

Parameter	Type	Description
code	String	Reason for the status of an access preview.

Example Requests

Obtaining access preview details

```
GET https://{hostname}/v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}
```

Example Responses

Status code: 200

OK

```
{
  "access_preview" : {
    "analyzer_id" : "{analyzer_id}",
    "configurations" : {
      "iam_agency" : {
        "trust_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Condition\":{\"StringMatch\":{\"g:PrincipalOrgId
\":[\"org_id\"]}},\"Action\":[\"sts:agencies:assume\",\"sts::tagSession\",\"sts::setSourceIdentity\"],\"Effect
\":\"Allow\",\"Principal\":{\"IAM\":[\"dd...\"]}}]}"
      }
    },
    "created_at" : "2023-09-07T07:26:23.440Z",
    "access_preview_id" : "{access_preview_id}",
```



```
    "status" : "completed"
  }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.4.4 Obtaining Findings Generated for an Access Preview

Function

This API is used to obtain the findings generated for an access preview.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:listPreviewFindings	List	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

POST /v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}/findings

Table 4-519 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Parameter	Mandatory	Type	Description
access_preview_id	Yes	String	Unique identifier of an access preview. Minimum: **1** Maximum: **36**

Request Parameters

Table 4-520 Request body parameters

Parameter	Mandatory	Type	Description
filters	No	Array of **FindingFilter** objects	A filter to match the returned findings. Array Length: **1 - 20**
limit	No	Integer	Maximum number of results on a page
marker	No	String	Page marker

Table 4-521 FindingFilter

Parameter	Mandatory	Type	Description
criterion	Yes	**Criterion** object	Criteria in the filter. Only one operator is allowed.

Parameter	Mandatory	Type	Description
key	Yes	String	Filter key. • **resource**: resource URN • **resource_type**: resource type • **resource_owner_account**: resource owner account • **is_public**: public access permission • **id**: finding ID • **status**: finding type • **principal_type** • **principal_identifier** • **change_type**: finding status change • **existing_finding_id**: ID of an existing finding • **existing_finding_status**: status of an existing finding • **condition.g:PrincipalUrn**: principal URN • **condition.g:PrincipalId**: principal ID • **condition.g:PrincipalAccount**: principal account • **condition.g:PrincipalOrgId**: principal organization ID • **condition.g:PrincipalOrgPath**: principal organization path • **condition.g:PrincipalOrgManagementAccountId**: principal organization management account ID • **condition.g:SourceIp**: source IP address • **condition.g:SourceVpc**: source VPC • **condition.g: SourceVpce**: source VPC endpoint • **finding_type**: finding type

Table 4-522 Criterion

Parameter	Mandatory	Type	Description
contains	No	Array of strings	Matching the "contains" operator in the filter Array Length: **1 - 20**
eq	No	Array of strings	Matching the "eq" operator in the filter Array Length: **1 - 20**
exists	No	Boolean	Matching the "exists" operator in the filter
neq	No	Array of strings	Matching the "neq" operator in the filter Array Length: **1 - 20**

Response Parameters

Status code: 200

Table 4-523 Response body parameters

Parameter	Type	Description
findings	Array of **PreviewFinding** objects	List of findings generated by an access preview.
page_info	**PageInfo** object	Information on the page

Table 4-524 PreviewFinding

Parameter	Type	Description
action	Array of strings	Action that can be used by external principals.
change_type	String	Finding change. • **unchanged**: no change • **new**: new content • **changed**: content updated
condition	Array of **FindingCondition** objects	Condition that generates findings for an access preview in the policy statement.

Parameter	Type	Description
created_at	String	Time when the findings were generated for an access preview.
existing_finding_id	String	Unique identifier of a finding.
existing_finding_status	String	Finding status. • **active** • **archived** • **resolved**
id	String	Unique identifier of a finding.
is_public	Boolean	Whether the policy that generates findings allows public access to resources.
principal	**FindingPrincipal** object	An external principal that accesses resources in a zone of trust.
resource	String	Unique identifier of a resource.
resource_owner_account	String	ID of the account that owns resources.
resource_type	String	Resource type. • **iam:agency**: IAM agency • **iam:user**: IAM user • **kms:cmk**: DEW shared key • **obs:bucket**: OBS bucket • **swr:repo**: SWR image repository • **cbr:backup**: CBR backup • **ims:image**: IMS image
sources	Array of strings	Source of findings, indicating how to grant access that generates the findings.
status	String	Status after the change. • **active** • **archived** • **resolved**

Table 4-525 FindingCondition

Parameter	Type	Description
key	String	Identifier or name of a condition key.

Parameter	Type	Description
value	String	Value of the condition key.

Table 4-526 FindingPrincipal

Parameter	Type	Description
identifier	String	Identifier of a principal.
type	String	Type of a principal. • **all_principal**: all principals • **account** • **all_user_in_account**: all users in an account • **all_agency_in_account**: all agencies in an account • **all_identity_provider_in_account**: all identity providers in an account • **specific_user**: specific user • **specific_agency**: specific agency • **specific_group**: specific user group • **specific_identity_provider**: specific identity provider

Table 4-527 PageInfo

Parameter	Type	Description
current_count	Integer	Number of items on the current page
next_marker	String	If present, it indicates that the available output is more than the output contained in the current response. Use this value in the marker request parameter in a subsequent call to the operation to get the next part of the output. You should repeat this operation until the **next_marker** response returns **null**.

Example Requests

Obtaining findings generated for an access preview

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}/findings
```

```
{
  "filters" : [ {
    "criterion" : {
      "eq" : [ "iam:agency" ]
    },
    "key" : "resource_type"
  } ]
}
```

Example Responses

Status code: 200

OK

```
{
  "findings" : [ {
    "action" : [ "sts::setSourceIdentity", "sts::tagSession", "sts:agencies:assume" ],
    "change_type" : "new",
    "condition" : [ {
      "key" : "g:PrincipalOrgId",
      "value" : "org_id"
    } ],
    "created_at" : "2023-09-07T07:26:23.440Z",
    "existing_finding_status" : null,
    "existing_finding_id" : null,
    "is_public" : false,
    "id" : "{finding_id}",
    "principal" : {
      "identifier" : "{domain_id}",
      "type" : "account"
    },
    "resource" : "iam::{domain_id}:agency:{agency_name}",
    "resource_owner_account" : "{domain_id}",
    "resource_type" : "iam:agency",
    "status" : "active"
  } ],
  "page_info" : {
    "current_count" : 1,
    "next_marker" : null
  }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.5 Tags

4.3.5.1 Deleting Tags from the Specified Resource

Function

This API is used to delete tags from the specified resource.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer::untagResource	Tagging	analyzer *	g:ResourceTag/<tag-key>	-	-
		-	g:TagKeys		

URI

POST /v5/{resource_type}/{resource_id}/tags/delete

Table 4-528 Path Parameters

Parameter	Mandatory	Type	Description
resource_type	Yes	String	Resource type. • **analyzers**: analyzer
resource_id	Yes	String	Unique identifier of a resource Minimum: **1** Maximum: **36**

Request Parameters

Table 4-529 Request body parameters

Parameter	Mandatory	Type	Description
tag_keys	Yes	Array of strings	List of tag keys to be deleted. Array Length: **1 - 20**

Response Parameters

Status code: 200

OK

None

Example Requests

Deleting tags from the specified resource

```
POST https://{hostname}/v5/{resource_type}/{resource_id}/tags/delete

{
  "tag_keys" : [ "key-1" ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.5.2 Adding Tags to the Specified Resource

Function

This API is used to add tags to the specified resource.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer::tagResource	Tagging	analyzer *	g:ResourceTag/<tag-key>	-	-

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
		-	• g:RequestTag/<tag-key> • g:TagKeys		

URI

POST /v5/{resource_type}/{resource_id}/tags/create

Table 4-530 Path Parameters

Parameter	Mandatory	Type	Description
resource_type	Yes	String	Resource type. • **analyzers**: analyzer
resource_id	Yes	String	Unique identifier of a resource Minimum: **1** Maximum: **36**

Request Parameters

Table 4-531 Request body parameters

Parameter	Mandatory	Type	Description
tags	Yes	Array of **Tag** objects	List of custom tags. Array Length: **1 - 20**

Table 4-532 Tag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key
value	Yes	String	String value associated with the tag key.

Response Parameters

Status code: 200

OK

None

Example Requests

Adding a tag to the specified resource

```
POST https://{hostname}/v5/{resource_type}/{resource_id}/tags/create

{
  "tags" : [ {
    "key" : "key-1",
    "value" : "value-1"
  } ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.6 Policy Validation

4.3.6.1 Validating a Policy

Function

This API is used to validate a policy and return a list of findings.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer::validatePolicy	Read	-	-	-	-

URI

POST /v5/policies/validate

Table 4-533 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results on a page Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Page marker Minimum: **4** Maximum: **400**

Request Parameters

Table 4-534 Request header parameters

Parameter	Mandatory	Type	Description
X-Language	No	String	Language of the returned message. The default value is 'zh-cn'. • **zh-cn**: Chinese • **en-us**: English Default: **zh-cn**

Table 4-535 Request body parameters

Parameter	Mandatory	Type	Description
policy_document	Yes	String	JSON policy document.

Parameter	Mandatory	Type	Description
policy_type	Yes	String	Type of the policy to be validated. • **identity_policy**: identity policy • **resource_policy**: resource policy • **service_control_policy**: service control policy • **resource_control_policy**: resource control policy • **network_control_policy**: network control policy
validate_policy_resource_type	No	String	The type of resource to attach to your resource policy. • **iam:agency**: IAM agency

Response Parameters

Status code: 200

Table 4-536 Response body parameters

Parameter	Type	Description
findings	Array of **ValidatePolicyFinding** objects	Actionable recommendation that can be used to improve the policy.
page_info	**PageInfo** object	Information on the page

Table 4-537 ValidatePolicyFinding

Parameter	Type	Description
finding_details	String	A localized message that explains the finding and provides guidance on how to address it

Parameter	Type	Description
finding_type	String	Impact level. • **security_warning**: There are security risks, which may be caused by overly permissive access. • **error**: There are errors that prevent the policy from functioning, such as syntax errors or invalid parameters. If an error occurs, the policy cannot be created. • **warning**: There are warnings that prevent the policy from functioning, such as a mismatch between a parameter type and a value. The policy can still be created even if there is a warning. • **suggestion**: There are suggestions for the policy to achieve expected results. For example, suggestions are given when there are empty arrays or empty objects.
issue_code	String	Provides an identifier of the issue associated with the validation check findings.
learn_more_link	String	Links to related documents associated with the validation check findings.
locations	Array of **Location** objects	List of locations that are related to the validation check findings in the policy document.

Table 4-538 Location

Parameter	Type	Description
path	Array of **PathElement** objects	A path in a policy, represented as a sequence of path elements
span	**Span** object	Span of the cursor in a policy, consisting of a start position (inclusive) and end position (exclusive)

Table 4-539 PathElement

Parameter	Type	Description
index	Integer	Index in a JSON array, starting from 0
key	String	Key in a JSON object
substring	**Substring** object	Substring of a literal string in a JSON object
value	String	Value associated with a given key in a JSON object

Table 4-540 Substring

Parameter	Type	Description
start	Integer	Start index of the substring, starting from 0. The value **0** indicates the first character.
length	Integer	Length of the substring

Table 4-541 Span

Parameter	Type	Description
start	**Position** object	Position in a policy
end	**Position** object	Position in a policy

Table 4-542 Position

Parameter	Type	Description
line	Integer	Line of the position, starting from 1
column	Integer	Column of the position, starting from 0.
offset	Integer	Offset within the policy that corresponds to the position, starting from 0.

Table 4-543 PageInfo

Parameter	Type	Description
current_count	Integer	Number of items on the current page
next_marker	String	If present, it indicates that the available output is more than the output contained in the current response. Use this value in the marker request parameter in a subsequent call to the operation to get the next part of the output. You should repeat this operation until the **next_marker** response returns **null**.

Example Requests

Requesting the validation of a policy and returning a list of findings

```
POST https://{hostname}/v5/policies/validate

{
  "policy_document" : "",
  "policy_type" : "identity_policy"
}
```

Example Responses

Status code: 200

OK

```
{
  "findings" : [ {
    "finding_details" : "Fix the JSON syntax error in row 1 and column 0 of index 0.",
    "finding_type" : "error",
    "issue_code" : "JSON_SYNTAX_ERROR",
    "learn_more_link" : "https://{endpoint}/section0",
    "locations" : [ {
      "path" : [ ],
      "span" : {
        "start" : {
          "line" : 1,
          "column" : 0,
          "offset" : 0
        },
        "end" : {
          "line" : 1,
          "column" : 1,
          "offset" : 1
        }
      }
    } ]
  } ],
  "page_info" : {
    "current_count" : 1,
    "next_marker" : null
  }
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.6.2 Checking Whether a Policy Has New Access

Function

This API is used to check whether a policy has new access.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer::checkNoNewAccess	Read	-	-	-	-

URI

POST /v5/policies/check-no-new-access

Request Parameters

Table 4-544 Request body parameters

Parameter	Mandatory	Type	Description
existing_policy_document	Yes	String	JSON policy document.
new_policy_document	Yes	String	JSON policy document.

Parameter	Mandatory	Type	Description
policy_type	Yes	String	Type of the policy to be validated. • **identity_policy**: identity policy • **agency_trust_policy**: agency trust policy • **bucket_policy**: bucket policy

Response Parameters

Status code: 200

Table 4-545 Response body parameters

Parameter	Type	Description
message	String	Whether the updated policy allows new access.
check_result	String	Findings generated for the new access. • **pass**: There are no new access permissions. • **fail**: New access permissions are added.
reasons	Array of **CheckNoNewAccessReason** objects	Statement description of a new action.

Table 4-546 CheckNoNewAccessReason

Parameter	Type	Description
description	String	Description of the inference on the check findings.
statement_id	String	SID of the new permission statement.
statement_index	Integer	Index of the new permission statement, starting from 0. Minimum: **0**

Example Requests

Checking whether a policy has new access


```
POST https://{hostname}/v5/policies/check-no-new-access

{
  "existing_policy_document" : "{\\\"Version\\\":\\\"5.0\\\",\\\"Statement\\\":[{\\\"Effect\\\":\\\"Allow\\\",\\
\"Action\\\":[\\\"iam:users:createUserV5\\\"]}]}",
  "new_policy_document" : "{\\\"Version\\\":\\\"5.0\\\",\\\"Statement\\\":[{\\\"Effect\\\":\\\"Allow\\\",\\
\"Action\\\":[\\\"iam:users:createUserV5\\\",\\\"obs:bucket:createBucket\\\"]}]}",
  "policy_type" : "identity_policy"
}
```

Example Responses

Status code: 200

OK

```
{
  "check_result" : "fail",
  "message" : "The modified permissions grant new access compared to your existing policy.",
  "reasons" : [ {
    "description" : "New access in the statement with sid: {statement_sid}.",
    "statement_index" : 0,
    "statement_id" : "{statement_sid}"
  } ]
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.7 Resource Analysis Configuration

4.3.7.1 Listing Resource Analysis Configurations

Function

This API is used to list the resource analysis configuration of a specified analyzer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:listResourceConfigurations	List	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

GET /v5/analyzers/{analyzer_id}/resource-configurations

Table 4-547 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Table 4-548 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results on a page Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Page marker Minimum: **4** Maximum: **400**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-549 Response body parameters

Parameter	Type	Description
resource_configurations	Array of **ResourceConfiguration** objects	Resource configuration in privilege escalation access.
page_info	**PageInfo** object	Information on the page

Table 4-550 ResourceConfiguration

Parameter	Type	Description
resource	String	Unique identifier of a resource.
actions	Array of strings	List of operations to be analyzed for the current resource. Array Length: **1 - 500**

Table 4-551 PageInfo

Parameter	Type	Description
current_count	Integer	Number of items on the current page
next_marker	String	If present, it indicates that the available output is more than the output contained in the current response. Use this value in the marker request parameter in a subsequent call to the operation to get the next part of the output. You should repeat this operation until the **next_marker** response returns **null**.

Status code: 400

Table 4-552 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 403

Table 4-553 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 404

Table 4-554 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Example Requests

Listing the resource analysis configuration of a specified analyzer

```
GET https://{hostname}/v5/analyzers/{analyzer_id}/resource-configurations
```

Example Responses

Status code: 200

OK

```
{
  "resource_configurations" : [ {
    "resource" : "iam::{domain_id}:agency:{agency_name}",
    "actions" : [ "iam:agencies:update" ]
  } ],
  "page_info" : {
    "current_count" : 1,
    "next_marker" : null
  }
}
```


Status Codes

Status Code	Description
200	OK
400	Bad request
403	Forbidden
404	Not found

Error Codes

See **Error Codes**.

4.3.7.2 Creating the Resource Analysis Configuration

Function

This API is used to create the resource analysis configuration of a specified analyzer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:createResourceConfigurations	Write	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

POST /v5/analyzers/{analyzer_id}/resource-configurations/create

Table 4-555 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Request Parameters

Table 4-556 Request body parameters

Parameter	Mandatory	Type	Description
resource_configurations	Yes	Array of **ResourceConfiguration** objects	Resource configuration in privilege escalation access. Array Length: **1 - 20**

Table 4-557 ResourceConfiguration

Parameter	Mandatory	Type	Description
resource	Yes	String	Unique identifier of a resource.
actions	Yes	Array of strings	List of operations to be analyzed for the current resource. Array Length: **1 - 500**

Response Parameters

Status code: 200

OK

Status code: 400

Table 4-558 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Parameter	Type	Description
encoded_authorization_message	String	Authentication information.

Status code: 403

Table 4-559 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 404

Table 4-560 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 409

Table 4-561 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Example Requests

Creating the resource analysis configuration of a specified analyzer

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/resource-configurations/create

{
  "resource_configurations" : [ {
    "resource" : "iam::{domain_id}:agency:{agency_name}",
    "actions" : [ "iam:agencies:update" ]
  } ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Bad request
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.3.7.3 Deleting the Resource Analysis Configuration

Function

This API is used to delete the resource analysis configuration of a specified analyzer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:analyzer:deleteResourceConfigurations	Write	analyzer *	g:ResourceTag/<tag-key>	-	-

URI

POST /v5/analyzers/{analyzer_id}/resource-configurations/delete

Table 4-562 Path Parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer Minimum: **1** Maximum: **36**

Request Parameters

Table 4-563 Request body parameters

Parameter	Mandatory	Type	Description
resources	Yes	Array of strings	List of resources to be deleted. Array Length: **1 - 20**

Response Parameters

Status code: 200

OK

Status code: 400

Table 4-564 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Parameter	Type	Description
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 403

Table 4-565 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 404

Table 4-566 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 409

Table 4-567 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.

Parameter	Type	Description
encoded_authorization_message	String	Authentication information.

Example Requests

Deleting the resource analysis configuration of a specified analyzer

```
POST https://{hostname}/v5/analyzers/{analyzer_id}/resource-configurations/delete

{
  "resources" : [ "iam::{domain_id}:agency:{agency_name}" ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Bad request
403	Forbidden
404	Not found
409	Conflict

Error Codes

See **Error Codes**.

4.3.8 Message Notification Configuration

4.3.8.1 Obtaining the Message Notification Configuration List

Function

This API is used to obtain the message notification configuration list.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:notificationSetting:list	Read	notificationSetting *	-	-	-

URI

GET /v5/notification-settings

Table 4-568 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results on a page Minimum: **1** Maximum: **200** Default: **100**
marker	No	String	Page marker Minimum: **4** Maximum: **400**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-569 Response body parameters

Parameter	Type	Description
notification_settings	Array of **NotificationSettingSummary** objects	Message notification configuration list.
page_info	**PageInfo** object	Information on the page

Table 4-570 NotificationSettingSummary

Parameter	Type	Description
id	String	Unique identifier of the message notification configuration.
urn	String	Unique resource identifier of the message notification configuration.
analyzer_id	String	Unique identifier of an analyzer
analyzer_name	String	Name of an analyzer
analyzer_type	String	Type of an access analyzer. • **account**: account-level external access analyzer • **organization**: organization-level external access analyzer • **account_unused_access**: account-level unused access analyzer • **organization_unused_access**: organization-level unused access analyzer • **account_privilege_escalation**: account-level privilege escalation access analyzer • **account_iam_best_practice**: account-level IAM best practice analyzer
mc_switch	Boolean	Whether to enable message notifications.
smn_topic_urns	Array of strings	URN list of SMN topics configured for message notifications.
created_at	String	Time when the message notification configuration is created.
updated_at	String	Time when the message notification configuration was last updated.

Table 4-571 PageInfo

Parameter	Type	Description
current_count	Integer	Number of items on the current page

Parameter	Type	Description
next_marker	String	If present, it indicates that the available output is more than the output contained in the current response. Use this value in the marker request parameter in a subsequent call to the operation to get the next part of the output. You should repeat this operation until the **next_marker** response returns **null**.

Status code: 400

Table 4-572 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 403

Table 4-573 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Example Requests

Obtaining the message notification configuration list

```
GET https://{hostname}/v5/notification-settings
```


Example Responses

Status code: 200

OK


```
{
  "notification_settings" : [ {
    "id" : "{notification_setting_id}",
    "urn" : "AccessAnalyzer:{region_id}:{domain_id}:notificationSetting:{notification_setting_id}",
    "analyzer_id" : "3de500b3f6c74b0a8ef170656f8a6376",
    "analyzer_type" : "account",
    "analyzer_name" : "external_analyzer_1",
    "mc_switch" : true,
    "smn_topic_urns" : [ "urn:smn:cn-north-7:******:test1" ],
    "created_at" : "2023-09-07T08:04:41.698Z",
    "updated_at" : "2023-09-07T08:04:41.698Z"
  }, {
    "id" : "{notification_setting_id}",
    "urn" : "AccessAnalyzer:{region_id}:{domain_id}:notificationSetting:{notification_setting_id}",
    "analyzer_id" : "7d866d909fda4e32b1fc2aae45c34a97",
    "analyzer_type" : "account",
    "analyzer_name" : "external_analyzer_2",
    "mc_switch" : true,
    "smn_topic_urns" : [ "urn:smn:cn-north-7:******:test1" ],
    "created_at" : "2023-09-07T08:04:41.698Z",
    "updated_at" : "2023-09-07T08:04:41.698Z"
  } ],
  "page_info" : {
    "current_count" : 2,
    "next_marker" : null
  }
}
```


Status Codes

Status Code	Description
200	OK
400	Bad request
403	Forbidden

Error Codes

See **Error Codes**.

4.3.8.2 Creating a Message Notification Configuration

Function

This API is used to create a message notification configuration.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:notificationSetting:create	Write	notificationSetting *	-	-	-

URI

POST /v5/notification-settings

Request Parameters

Table 4-574 Request body parameters

Parameter	Mandatory	Type	Description
analyzer_id	Yes	String	Unique identifier of an analyzer
mc_switch	Yes	Boolean	Whether to enable message notifications.
smn_topic_urns	Yes	Array of strings	URN list of SMN topics configured for message notifications.

Response Parameters

Status code: 201

Table 4-575 Response body parameters

Parameter	Type	Description
id	String	Unique identifier of the message notification configuration.
urn	String	Unique resource identifier of the message notification configuration.

Status code: 400

Table 4-576 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 403

Table 4-577 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 404

Table 4-578 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Example Requests

Creating a message notification configuration

```
POST https://{hostname}/v5/notification-settings

{
```

```
  "analyzer_id" : "3de500b3f6c74b0a8ef170656f8a6376",
  "mc_switch" : true,
  "smn_topic_urns" : [ "urn:smn:cn-north-7:******:test1" ]
}
```

Example Responses

Status code: 201

Created

```
{
  "id" : "1c8b66cc466943ad9f6238a19f6f6679"
}
```

Status Codes

Status Code	Description
201	Created
400	Bad request
403	Forbidden
404	NotFound

Error Codes

See **Error Codes**.

4.3.8.3 Obtaining a Message Notification Configuration

Function

This API is used to obtain a message notification configuration.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:notificationSetting:get	Read	notificationSetting *	-	-	-

URI

GET /v5/notification-settings/{notification_setting_id}

Table 4-579 Path Parameters

Parameter	Mandatory	Type	Description
notification_setting_id	Yes	String	Unique identifier of the message notification configuration. Minimum: **1** Maximum: **36**

Request Parameters

None

Response Parameters

Status code: 200

Table 4-580 Response body parameters

Parameter	Type	Description
id	String	Unique identifier of the message notification configuration.
urn	String	Unique resource identifier of the message notification configuration.
analyzer_id	String	Unique identifier of an analyzer
analyzer_name	String	Name of an analyzer

Parameter	Type	Description
analyzer_type	String	Type of an access analyzer. • **account**: account-level external access analyzer • **organization**: organization-level external access analyzer • **account_unused_access**: account-level unused access analyzer • **organization_unused_access**: organization-level unused access analyzer • **account_privilege_escalation**: account-level privilege escalation access analyzer • **account_iam_best_practice**: account-level IAM best practice analyzer
mc_switch	Boolean	Whether to enable message notifications.
smn_topic_urns	Array of strings	URN list of SMN topics configured for message notifications.
created_at	String	Time when the message notification configuration is created.
updated_at	String	Time when the message notification configuration was last updated.

Status code: 400

Table 4-581 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 403

Table 4-582 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 404

Table 4-583 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Example Requests

Obtaining a message notification configuration

```
GET https://{hostname}/v5/notification-settings/{notification_setting_id}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "{notification_setting_id}",
  "urn" : "AccessAnalyzer:{region_id}:{domain_id}:notificationSetting:{notification_setting_id}",
  "analyzer_id" : "3de500b3f6c74b0a8ef170656f8a6376",
  "analyzer_type" : "account",
  "analyzer_name" : "external_analyzer_1",
  "mc_switch" : true,
  "smn_topic_urns" : [ "urn:smn:cn-north-7:******:test1" ],
  "created_at" : "2023-09-07T08:04:41.698Z",
  "updated_at" : "2023-09-07T08:04:41.698Z"
}
```


Status Codes

Status Code	Description
200	OK
400	Bad request
403	Forbidden
404	NotFound

Error Codes

See **Error Codes**.

4.3.8.4 Updating a Message Notification Configuration

Function

This API is used to update a message notification configuration.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:notificationSetting:update	Write	notificationSetting *	-	-	-

URI

PUT /v5/notification-settings/{notification_setting_id}

Table 4-584 Path Parameters

Parameter	Mandatory	Type	Description
notification_setting_id	Yes	String	Unique identifier of the message notification configuration. Minimum: **1** Maximum: **36**

Request Parameters

Table 4-585 Request body parameters

Parameter	Mandatory	Type	Description
mc_switch	Yes	Boolean	Whether to enable message notifications.
smn_topic_urns	Yes	Array of strings	URN list of SMN topics configured for message notifications.

Response Parameters

Status code: 200

OK

Status code: 400

Table 4-586 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 403

Table 4-587 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 404

Table 4-588 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Example Requests

Updating a message notification configuration

```
POST https://{hostname}/v5/notification-settings/{notification_setting_id}

{
  "mc_switch" : true,
  "smn_topic_urns" : [ "urn:smn:cn-north-7:******:test1" ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Bad request
403	Forbidden

Status Code	Description
404	NotFound

Error Codes

See **Error Codes**.

4.3.8.5 Deleting a Message Notification Configuration

Function

This API is used to delete a message notification configuration.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the following required identity policy-based permissions. For details about the required permissions, see **Permissions Policies and Supported Actions**.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
AccessAnalyzer:notificationSetting:delete	Write	notificationSetting *	-	-	-

URI

DELETE /v5/notification-settings/{notification_setting_id}

Table 4-589 Path Parameters

Parameter	Mandatory	Type	Description
notification_setting_id	Yes	String	Unique identifier of the message notification configuration. Minimum: **1** Maximum: **36**

Request Parameters

None

Response Parameters

Status code: 204

Deleted

Status code: 400

Table 4-590 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Status code: 403

Table 4-591 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Request ID.
encoded_authorization_message	String	Authentication information.

Example Requests

This API is used to delete a message notification configuration.

```
POST https://{hostname}/v5/notification-settings/{notification_setting_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	Deleted

Status Code	Description
400	Bad request
403	Forbidden

Error Codes

See **Error Codes**.

5 Example Applications

5.1 Periodic Rotation of Access Keys

Scenario

Enterprise users usually use access keys (AK/SKs) to access cloud resources through APIs. They are advised to make access keys automatically rotate to reduce potential security risks.

This section guides you through rotating access keys by calling APIs. You can also automate rotation of access keys using programmatic methods.

General Procedure

The following steps are involved to periodically rotate your access keys:

1. Create an access key.
2. Query the time when all of your access keys are created, and determine whether they need to be rotated.
3. Create an access key.
4. Delete the old access key.

The following APIs will be used in this example:

- **Creating a Permanent Access Key**
- **Querying Permanent Access Keys**
- **Deleting a Permanent Access Key**

Step 1: Create a Permanent Access Key

URI: POST /v5/users/{user_id}/access-keys

For details about the API, see **Creating a Permanent Access Key**.

- Example Request
  POST https://{endpoint}/v5/users/07609fb9358010e21f7bc003751.../access-keys

- Example Response

```
{
  "access_key" : {
    "user_id" : "07609fb9358010e21f7bc003751...",
    "access_key_id" : "P83EVBZJMXCYTMUII...",
    "created_at" : "2023-09-13T06:51:20.550Z",
    "secret_access_key" : "TTqAHPbhWorg9ozx8Dv9MUyzYnOKDppxzHt...",
    "status" : "active"
  }
}
```

Step 2: Query the Creation Time of All Access Keys

URI: GET /v5/users/{user_id}/access-keys

For details about the API, see **Querying Permanent Access Keys**.

- Example Request

```
GET https://{endpoint}/v5/users/07609fb9358010e21f7bc003751.../access-keys
```

- Example Response

```
{
  "access_keys" : [ {
    "user_id" : "07609fb9358010e21f7bc003751...",
    "access_key_id" : "P83EVBZJMXCYTMUII...",
    "created_at" : "2023-09-13T06:51:20.550Z",
    "status" : "active"
  } ],
  "page_info" : {
    "current_count" : 1
  }
}
```

Step 3: Create a New Access Key

Repeat **Step 1: Create a Permanent Access Key**.

Step 4: Delete the Old Access Key

URI: DELETE /v5/users/{user_id}/access-keys/{access_key_id}

For details about the API, see **Deleting a Permanent Access Key**.

- Example Request

```
DELETE https://{endpoint}/v5/users/07609fb9358010e21f7bc003751.../access-keys/
P83EVBZJMXCYTMUII...
```

- Example Response

  This API does not have a response body. If the status code **204** is displayed, the access key is deleted successfully.

5.2 Security Auditing on Permissions of IAM Users

Scenario

Enterprise users usually need to periodically audit the permissions of IAM users created in the cloud, ensuring that IAM users only have the permissions required to complete certain tasks. Generally, only account administrators and auditors have administration permissions for the IAM service, and IAM users should not

have these permissions. Periodic security audit can be automatically implemented through APIs.

This section describes how to perform security audit on the permissions of IAM users by calling APIs. You can also implement periodic security audit using programmatic methods.

General Procedure

You can perform security audit on the permissions of IAM users, including identity policies attached to IAM users and IAM user groups. You can perform permission audit on the identity policies attached to IAM users by comparing the permissions to be audited with the content of the attached identity policies. The following uses identity policies attached to IAM user groups as an example to describe how to audit permissions. The procedure is as follows:

1. List all the user groups.
2. Query the permissions of each user group.
3. Query the content of an identity policy.
4. Determine the permissions to be audited and query the IAM users in each user group that has been assigned these permissions.

The following APIs will be used in this example:

- **Listing User Groups**
- **Querying All Identity Policies Attached to a Specified User Group**
- **Querying All Versions of a Specified Identity Policy**
- **Querying the IAM Users in a Group**

Step 1: List All the User Groups

URI: GET /v5/groups

For details about the API, see **Listing User Groups**.

- Example Request

```
GET https://{endpoint}/v5/groups
```

- Example Response

```
{
  "groups" : [ {
    "group_id" : "5b050baea9db472c88cbae67e8d6....",
    "group_name" : "IAMGroupA",
    "created_at" : "2023-09-11T10:13:25.414Z",
    "urn" : "iam::d78cbac186b744899480f25bd022....:group:IAMGroupA",
    "description" : "IAMdescription"
  }, {
    "group_id" : "07609e7eb200250a3f7dc003cb7a....",
    "group_name" : "IAMGroupB",
    "created_at" : "2023-09-11T10:13:40.016Z",
    "urn" : "iam::d78cbac186b744899480f25bd022....:group:IAMGroupB",
    "description" : "IAMdescription"
  } ],
  "page_info" : {
    "current_count" : 2
  }
}
```


Step 2: Query Permissions of Each User Group

URI: GET /v5/groups/{group_id}/attached-policies

For details about the API, see **Querying All Identity Policies Attached to a Specified User Group**.

- Example Request
  GET https://{endpoint}/v5/groups/5b050baea9db472c88cbae67e8d6..../attached-policies
- Example Response

```
{
  "attached_policies" : [ {
    "policy_name" : "ReadPolicy",
    "policy_id" : "75cfe22af2b3498d82b655fbb39d....",
    "urn" : "iam::d78cbac186b744899480f25bd022.....:policy:ReadPolicy",
    "attached_at" : "2023-09-25T09:31:44.935Z"
  } ],
  "page_info" : {
    "current_count" : 1
  }
}
```

Step 3: Query the Content of an Identity Policy

URI: GET /v5/policies/{policy_id}/versions

For details about the API, see **Querying All Versions of a Specified Identity Policy**.

- Example Request
  GET https://{endpoint}/v5/policies/75cfe22af2b3498d82b655fbb39d..../versions
- Example Response

```
{
  "versions" : [ {
    "document" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"iam:*:get*
\",\"iam:*:list*\"]}]}",
    "version_id" : "v1",
    "is_default" : true,
    "created_at" : "2023-09-25T09:03:24.786Z"
  } ],
  "page_info" : {
    "current_count" : 1
  }
}
```

Step 4: Determine the Permissions to Be Audited and Query IAM Users Granted These Permissions

URI: GET /v5/users

For details about the API, see **Querying the IAM Users in a Group**.

- Example Request
  GET https://{endpoint}/v5/users?group_id=5b050baea9db472c88cbae67e8d6....
- Example Response

```
{
  "users" : [ {
    "description" : "description",
    "user_name" : "IAMUserA",
    "is_root_user" : false,
    "created_at" : "2023-04-26T03:49:42Z",
```



```
    "user_id" : "07609fb9358010e21f7bc003751c....",
    "urn" : "iam::d78cbac186b744899480f25bd022.....:user:IAMUserA",
    "enabled" : true
  }, {
    "description" : "description",
    "user_name" : "IAMUserB",
    "is_root_user" : false,
    "created_at" : "2023-04-26T03:52:27Z",
    "user_id" : "076837351e80251c1f0fc003afe4....",
    "urn" : "iam::d78cbac186b744899480f25bd022.....:user:IAMUserB",
    "enabled" : true
  } ],
  "page_info" : {
    "current_count" : 2
  }
}
```


6 Permissions and Supported Actions

6.1 Permissions and Supported Actions

You can use Identity and Access Management (IAM) for fine-grained permissions management of your IAM resources. If your HUAWEI ID does not need individual IAM users, you can skip this section.

With IAM, you can control access to specific Huawei Cloud resources.

IAM supports role/policy-based authorization and identity policy-based authorization.

The following table describes the differences between these two authorization models.

Table 6-1 Differences between role/policy-based and identity policy-based authorization

Authorization Model	Core Relationship	Permissions	Authorization Method	Description
Role/Policy	User-permission-authorization scope	• System-defined roles • System-defined policies • Custom policies	Assigning roles or policies to identities	To authorize a user, you need to add it to a user group first and then specify the scope of authorization. It provides a limited number of condition keys and cannot meet the requirements of fine-grained permissions control. This method is suitable for small- and medium-sized enterprises.

Authorization Model	Core Relationship	Permissions	Authorization Method	Description
Identity policy	User-policy	• System-defined identity policies • Custom identity policies	• Granting permissions of identity policies to identities • Attaching identity policies to identities	You can authorize a user by attaching an identity policy to it. User-specific authorization and a variety of key conditions allow for more fine-grained permissions control. However, this model can be hard to set up. It requires a certain amount of expertise and is suitable for medium- and large-sized enterprises.

Policies/identity policies and actions in the two authorization models are not interoperable. You are advised to use the identity policy-based authorization model.

If you use IAM users in your account to call an API, the IAM users must be granted the required permissions. The required permissions are determined by the actions supported by the API. Only users with the policies allowing for those actions can call the API successfully.

6.2 IAM Identity Policy-based Authorization Reference

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the **Organizations** service also provides **Service Control Policies (SCPs)** to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see **How IAM Is Different from Organizations for Access Control?**.

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see **Creating a Custom Identity Policy**.
- For details about how to use these elements to edit a custom SCP, see **Creating an SCP**.

Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

  For details about the resource types defined by IAM, see **Resources**.
- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

  For details about the condition keys defined by IAM, see **Conditions**.
- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see **Policies and Identity Policies**.

The following table lists the actions that you can define in identity policy statements for IAM.

Table 6-2 Actions supported by IAM

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam::listAccessKeys	Grants permission to list permanent access keys.	List	-	-	• iam:credentials:listCredentials
iam::createAccessKey	Grants permission to create a permanent access key.	Write	-	-	• iam:credentials:createCredential
iam::getAccessKey	Grants permission to query a permanent access key.	Read	-	-	• iam:credentials:getCredential
iam::updateAccessKey	Grants permission to update a permanent access key.	Write	-	-	• iam:credentials:updateCredential
iam::deleteAccessKey	Grants permission to delete a permanent access key.	Write	-	-	• iam:credentials:deleteCredential
iam:projects:list	Grants permission to list projects.	List	-	-	• iam:projects:listProjects
iam:projects:create	Grants permission to create a project.	Write	-	-	• iam:projects:createProject
iam:projects:listForUser	Grants permission to list projects of a specified user.	List	-	-	• iam:projects:listProjectsForUser

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:projects:update	Grants permission to update a project.	Write	-	-	• iam:projects:updateProject
iam:groups:list	Grants permission to list groups.	List	-	-	• iam:groups:listGroups
iam:groups:create	Grants permission to create a group.	Write	-	-	• iam:groups:createGroup
iam:groups:get	Grants permission to query a group.	Read	-	-	• iam:groups:getGroup
iam:groups:delete	Grants permission to delete a group.	Write	-	-	• iam:groups:deleteGroup
iam:groups:update	Grants permission to update a group.	Write	-	-	• iam:groups:updateGroup
iam:groups:removeUser	Grants permission to remove user from a group.	Write	-	-	• iam:permissions:removeUserFromGroup
iam:groups:listUsers	Grants permission to list users of a specified group.	List	-	-	• iam:users:listUsersForGroup
iam:groups:checkUser	Grants permission to query whether a user is in the group.	Read	-	-	• iam:permissions:checkUserInGroup

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:groups:addUser	Grants permission to add user to a group.	Write	-	-	• iam:permissions:addUserToGroup
iam:users:create	Grants permission to create a user.	Write	-	-	• iam:users:createUser
iam:users:get	Grants permission to query a user.	Read	-	-	• iam:users:getUser
iam:users:update	Grants permission to update a user.	Write	-	-	• iam:users:updateUser
iam:users:list	Grants permission to list users.	List	-	-	• iam:users:listUsers
iam:users:delete	Grants permission to delete a user.	Write	-	-	• iam:users:deleteUser
iam:users:listGroups	Grants permission to list groups of a specified user.	List	-	-	• iam:groups:listGroupsForUser
iam:users:listVirtualMFADevices	Grants permission to list virtual MFA devices of a specified user.	List	-	-	• iam:mfa:listVirtualMFADevices
iam:users:createVirtualMFADevice	Grants permission to create a virtual MFA device.	Write	-	-	• iam:mfa:createVirtualMFADevice

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:users:deleteVirtualMFADevice	Grants permission to delete a virtual MFA device.	Write	-	-	• iam:mfa:deleteVirtualMFADevice
iam:users:getVirtualMFADevice	Grants permission to query a virtual MFA device.	Read	-	-	• iam:mfa:getVirtualMFADevice
iam:users:bindVirtualMFADevice	Grants permission to bind a virtual MFA device.	Write	-	-	• iam:mfa:bindMFADevice
iam:users:unbindVirtualMFADevice	Grants permission to unbind a virtual MFA device.	Write	-	-	• iam:mfa:unbindMFADevice
iam:identityProviders:list	Grants permission to list identity providers.	List	-	-	• iam:identityProviders:listIdentityProviders
iam:identityProviders:get	Grants permission to query an identity provider.	Read	-	-	• iam:identityProviders:getIdentityProvider
iam:identityProviders:create	Grants permission to create an identity provider.	Write	-	-	• iam:identityProviders:createIdentityProvider
iam:identityProviders:delete	Grants permission to delete an identity provider.	Write	-	-	• iam:identityProviders:deleteIdentityProvider

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:identityProviders:update	Grants permission to update an identity provider.	Write	-	-	• iam:identityProviders:updateIdentityProvider
iam:identityProviders:listMappings	Grants permission to list mappings of an identity provider.	List	-	-	-
iam:identityProviders:getMapping	Grants permission to query mapping of an identity provider.	Read	-	-	-
iam:identityProviders:createMapping	Grants permission to create mapping of an identity provider.	Write	-	-	-
iam:identityProviders:deleteMapping	Grants permission to delete mapping of an identity provider.	Write	-	-	-
iam:identityProviders:updateMapping	Grants permission to update mapping of an identity provider.	Write	-	-	-
iam:identityProviders:listProtocols	Grants permission to list protocols of an identity provider.	List	-	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:identityProviders:getProtocol	Grants permission to query protocol of an identity provider.	Read	-	-	-
iam:identityProviders:createProtocol	Grants permission to create protocol of an identity provider.	Write	-	-	-
iam:identityProviders:deleteProtocol	Grants permission to delete protocol of an identity provider.	Write	-	-	-
iam:identityProviders:updateProtocol	Grants permission to update a protocol of an identity provider.	Write	-	-	-
iam:identityProviders:getSAMLMetadata	Grants permission to query SAML metadata file of an identity provider.	Read	-	-	• iam:identityProviders:getIDPMetadata
iam:identityProviders:createSAMLMetadata	Grants permission to create SAML metadata file of an identity provider.	Write	-	-	• iam:identityProviders:createIDPMetadata

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:identityProviders:getOIDCConfig	Grants permission to query OIDC configuration of an identity provider.	Read	-	-	• iam:identityProviders:getOpenIDConnectConfig
iam:identityProviders:createOIDCConfig	Grants permission to create OIDC configuration of an identity provider.	Write	-	-	• iam:identityProviders:createOpenIDConnectConfig
iam:identityProviders:updateOIDCConfig	Grants permission to update OIDC configuration of an identity provider.	Write	-	-	• iam:identityProviders:updateOpenIDConnectConfig
iam:securityPolicies:getProtectPolicy	Grants permission to query an operation protection policy.	Read	-	-	-
iam:securityPolicies:updateProtectPolicy	Grants permission to update an operation protection policy.	Write	-	-	-
iam:securityPolicies:getPasswordPolicy	Grants permission to query a password policy.	Read	-	-	-
iam:securityPolicies:updatePasswordPolicy	Grants permission to update a password policy.	Write	-	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:securityPolicies:getLoginPolicy	Grants permission to query a login policy.	Read	-	-	-
iam:securityPolicies:updateLoginPolicy	Grants permission to update a login policy.	Write	-	-	-
iam:securityPolicies:getConsoleAclPolicy	Grants permission to query a console access policy.	Read	-	-	-
iam:securityPolicies:updateConsoleAclPolicy	Grants permission to modify a console access policy.	Write	-	-	-
iam:securityPolicies:getApiAclPolicy	Grants permission to query an API access policy.	Read	-	-	-
iam:securityPolicies:updateApiAclPolicy	Grants permission to update an API access policy.	Write	-	-	-
iam:securityPolicies:getPrivacyTransferPolicy	Grants permission to query a privacy transfer policy.	Read	-	-	-
iam:securityPolicies:updatePrivacyTransferPolicy	Grants permission to update a privacy transfer policy.	Write	-	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:users:listLoginProtectSettings	Grants permission to list user login protect settings of the domain.	List	-	-	• iam:users:listUserLoginProtects
iam:users:getLoginProtectSetting	Grants permission to get the login protect setting.	Read	-	-	• iam:users:getUserLoginProtect
iam:users:updateLoginProtectSetting	Grants permission to update the login protect setting.	Write	-	-	• iam:users:setUserLoginProtect
iam:quotas:list	Grants permission to list quotas.	List	-	-	• iam:quotas:listQuotas
iam:quotas:listForProject	Grants permission to list quotas of a specified project.	List	-	-	• iam:quotas:listQuotasForProject
iam:agencies:pass	Grants permission to pass an agency to a service.	Permission_management	agency *	-	-
iam:roles:list	Grants permission to list roles.	List	-	-	• iam:roles:listRoles
iam:roles:get	Grants permission to get role detail.	Read	-	-	• iam:roles:getRole

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam::listRoleAssignments	Grants permission to query tenant assignment records.	List	-	-	• iam:permissions:listRoleAssignments
iam:groups:listRolesOnDomain	Grants permission to query user group permissions in global services.	List	-	-	• iam:permissions:listRolesForGroupOnDomain
iam:groups:listRolesOnProject	Grants permission to query user group permissions in project services.	List	-	-	• iam:permissions:listRolesForGroupOnProject
iam:groups:grantRoleOnDomain	Grants permission to grant global service permissions to a user group.	Write	-	-	• iam:permissions:grantRoleToGroupOnDomain
iam:groups:grantRoleOnProject	Grants permission to grant project level service to a user group.	Write	-	-	• iam:permissions:grantRoleToGroupOnProject
iam:groups:checkRoleOnDomain	Grants permission to query whether a user group has global service permissions.	Read	-	-	• iam:permissions:checkRoleForGroupOnDomain

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:groups:checkRoleOnProject	Grants permission to query whether a user group has the project service permission.	Read	-	-	• iam:permissions:checkRoleForGroupOnProject
iam:groups:listRoles	Grants permission to query permissions of a user group.	List	-	-	• iam:permissions:listRolesForGroup
iam:groups:checkRole	Grants permission to query whether a user group has specified permissions.	Read	-	-	• iam:permissions:checkRoleForGroup
iam:groups:revokeRole	Grants permission to remove specified permissions from a user group.	Write	-	-	• iam:permissions:revokeRoleFromGroup
iam:groups:revokeRoleOnDomain	Grants permission to remove global service permissions from a user group.	Write	-	-	• iam:permissions:revokeRoleFromGroupOnDomain
iam:groups:revokeRoleOnProject	Grants permission to remove project service permissions from a user group.	Write	-	-	• iam:permissions:revokeRoleFromGroupOnProject

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:groups:grantRole	Grants permission to grant specified permissions to a user group.	Write	-	-	• iam:permissions:grantRoleToGroup
iam:roles:create	Grants permission to create custom policies.	Write	-	-	• iam:roles:createRole
iam:roles:update	Grants permission to create custom policies.	Write	-	-	• iam:roles:updateRole
iam:roles:delete	Grants permission to delete custom policies.	Write	-	-	• iam:roles:deleteRole
iam:agencies:list	Grants permission to list agencies.	List	-	-	• iam:agencies:listAgencies
iam:agencies:listSwitchAgencyHistories	Grants permission to list the history of switching agency.	List	-	-	-
iam:agencies:get	Grants permission to query agency details.	Read	-	-	• iam:agencies:getAgency
iam:agencies:create	Grants permission to create agency.	Write	-	-	• iam:agencies:createAgency
iam:agencies:update	Grants permission to modify agency.	Write	-	-	• iam:agencies:updateAgency

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:agencies:delete	Grants permission to delete agency.	Write	-	-	• iam:agencies:deleteAgency
iam:agencies:listRolesOnDomain	Grants permission to query global service permissions of an agency.	List	-	-	• iam:permissions:listRolesForAgencyOnDomain
iam:agencies:listRolesOnProject	Grants permission to query project permissions of an agency.	List	-	-	• iam:permissions:listRolesForAgencyOnProject
iam:agencies:grantRoleOnDomain	Grants permission to grant global service permissions to agencies.	Write	-	-	• iam:permissions:grantRoleToAgencyOnDomain
iam:agencies:grantRoleOnProject	Grants permission to grant project services permissions to agencies.	Write	-	-	• iam:permissions:grantRoleToAgencyOnProject
iam:agencies:checkRoleOnDomain	Grants permission to query whether an agency has global service permissions.	Read	-	-	• iam:permissions:checkRoleForAgencyOnDomain
iam:agencies:checkRoleOnProject	Grants permission to query whether an agency has project service permissions.	Read	-	-	• iam:permissions:checkRoleForAgencyOnProject

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:agencies:revokeRoleOnDomain	Grants permission to remove agency global service permissions.	Write	-	-	• iam:permissions:revokeRoleFromAgencyOnDomain
iam:agencies:revokeRoleOnProject	Grants permission to remove agency project service permissions.	Write	-	-	• iam:permissions:revokeRoleFromAgencyOnProject
iam:agencies:listRoles	Grants permission to list permissions of agency.	List	-	-	• iam:permissions:listRolesForAgency
iam:agencies:grantRole	Grants permission to grant the specified permissions to an agency.	Write	-	-	• iam:permissions:grantRoleToAgency
iam:agencies:checkRole	Grants permission to check whether an agency has specified permissions.	Read	-	-	• iam:permissions:checkRoleForAgency
iam:agencies:revokeRole	Grants permission to remove specified permissions of an agency.	Write	-	-	• iam:permissions:revokeRoleFromAgency

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam::listGroupsAssignedEnterpriseProject	Grants permission to query permissions of a user group associated with an enterprise project.	List	-	-	• iam:permissions:listGroupsOnEnterpriseProject
iam:groups:listRolesOnEnterpriseProject	Grants permission to query permissions of a user group associated with an enterprise project.	List	-	-	• iam:permissions:listRolesForGroupOnEnterpriseProject
iam:groups:grantRoleOnEnterpriseProject	Grants permission to grant permissions to a user group associated with an enterprise project.	Write	-	-	• iam:permissions:grantRoleToGroupOnEnterpriseProject
iam:groups:revokeRoleOnEnterpriseProject	Grants permission to delete permissions of a user group associated with an enterprise project.	Write	-	-	• iam:permissions:revokeRoleFromGroupOnEnterpriseProject

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:groups:listAssignedEnterpriseProjects	Grants permission to query enterprise projects of group.	List	-	-	• iam:permissions:listEnterpriseProjectsForGroup
iam:users:listAssignedEnterpriseProjects	Grants permission to query enterprise projects of user.	List	-	-	• iam:permissions:listEnterpriseProjectsForUser
iam::listUsersAssignedEnterpriseProject	Grants permission to query users directly associated with an enterprise project.	List	-	-	• iam:permissions:listUsersForEnterpriseProject
iam:users:listRolesOnEnterpriseProject	Grants permission to query permissions of a user directly associated with an enterprise project.	List	-	-	• iam:permissions:listRolesForUserOnEnterpriseProject
iam:users:grantRoleOnEnterpriseProject	Grants permission to grant permissions to an enterprise project based on users.	Write	-	-	• iam:permissions:grantRoleToUserOnEnterpriseProject

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:users:revokeRoleOnEnterpriseProject	Grants permission to delete permissions of a user directly associated with an enterprise project.	Write	-	-	• iam:permissions:revokeRoleFromUserOnEnterpriseProject
iam:agencies:grantRoleOnEnterpriseProject	Grants permission to grant permissions to an enterprise project based on agencies.	Write	-	-	• iam:permissions:grantRoleToAgencyOnEnterpriseProject
iam:agencies:revokeRoleOnEnterpriseProject	Grants permission to delete permissions of an agency associated with an enterprise project.	Write	-	-	• iam:permissions:revokeRoleFromAgencyOnEnterpriseProject
iam:mfa:listMFADevicesV5	Grants permission to list MFA devices.	List	mfa *	-	-
iam:mfa:createVirtualMFADeviceV5	Grants permission to create a virtual MFA device.	Write	mfa *	-	-
iam:mfa:deleteVirtualMFADeviceV5	Grants permission to delete a virtual MFA device.	Write	mfa *	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:mfa:enableV5	Grants permission to enable a MFA device.	Write	mfa *	-	-
iam:mfa:disableV5	Grants permission to disable a MFA device.	Write	mfa *	-	-
iam:securitypolicies:getPasswordPolicyV5	Grants permission to retrieve information about the password policy.	Read	-	-	-
iam:securitypolicies:updatePasswordPolicyV5	Grants permission to update the password policy.	Write	-	-	-
iam:securitypolicies:getLoginPolicyV5	Grants permission to retrieve information about the login policy.	Read	-	-	-
iam:securitypolicies:updateLoginPolicyV5	Grants permission to update the login policy.	Write	-	-	-
iam:credentials:listCredentialsV5	Grants permission to list permanent access keys for an IAM user.	List	user *	**g:ResourceTag/<tag-key>**	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:credentials:showAccessKeyLastUsedV5	Grants permission to retrieve information about when the specified access key was last used.	Read	user *	g:ResourceTag/<tag-key>	-
iam:credentials:createCredentialV5	Grants permission to create a permanent access key for an IAM user.	Write	user *	g:ResourceTag/<tag-key>	-
iam:credentials:updateCredentialV5	Grants permission to update a permanent access key for an IAM user.	Write	user *	g:ResourceTag/<tag-key>	-
iam:credentials:deleteCredentialV5	Grants permission to delete a permanent access key for an IAM user.	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:changePasswordV5	Grants permission to an IAM user to change own password.	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:showLoginProfileV5	Grants permission to retrieve information about the login profile of an IAM user.	Read	user *	g:ResourceTag/<tag-key>	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:users:createLoginProfileV5	Grants permission to create login profile for an IAM user.	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:updateLoginProfileV5	Grants permission to update login profile for an IAM user.	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:deleteLoginProfileV5	Grants permission to delete login profile for an IAM user.	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:listUsersV5	Grants permission to list IAM users.	List	user *	-	-
iam:users:getUserV5	Grants permission to retrieve information about an IAM user.	Read	user *	g:ResourceTag/<tag-key>	-
iam:users:showUserLastLoginV5	Grants permission to retrieve information about when the specified IAM user key was logined.	Read	user *	g:ResourceTag/<tag-key>	-
iam:users:createUserV5	Grants permission to create an IAM user.	Write	user *	-	-
iam:users:updateUserV5	Grants permission to update an IAM user.	Write	user *	g:ResourceTag/<tag-key>	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:users:deleteUserV5	Grants permission to delete an IAM user.	Write	user *	g:ResourceTag/<tag-key>	-
iam:groups:listGroupsV5	Grants permission to list groups.	List	group *	-	-
iam:groups:getGroupV5	Grants permission to retrieve information about a group.	Read	group *	-	-
iam:groups:createGroupV5	Grants permission to create a group.	Write	group *	-	-
iam:groups:updateGroupV5	Grants permission to update a group.	Write	group *	-	-
iam:groups:deleteGroupV5	Grants permission to delete a group.	Write	group *	-	-
iam:permissions:addUserToGroupV5	Grants permission to add an IAM user to a group.	Write	group *	-	-
iam:permissions:removeUserFromGroupV5	Grants permission to remove an IAM user from a group.	Write	group *	-	-
iam:policies:listV5	Grants permission to list identity policies.	List	policy *	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:policies:getV5	Grants permission to retrieve information about an identity policy.	Read	policy *	-	-
iam:policies:createV5	Grants permission to create a custom identity policy.	Permission_management	policy *	-	-
iam:policies:deleteV5	Grants permission to delete a custom identity policy.	Permission_management	policy *	-	-
iam:policies:listVersionsV5	Grants permission to list versions for an identity policy.	List	policy *	-	-
iam:policies:getVersionV5	Grants permission to retrieve information about a version of an identity policy.	Read	policy *	-	-
iam:policies:createVersionV5	Grants permission to create a new version for a custom identity policy.	Permission_management	policy *	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:policies:deleteVersionV5	Grants permission to delete a version for a custom identity policy.	Permission_management	policy *	-	-
iam:policies:setDefaultVersionV5	Grants permission to set default version for a custom identity policy.	Permission_management	policy *	-	-
iam:agencies:attachPolicyV5	Grants permission to attach an identity policy to an agency or a trust agency.	Permission_management	agency *	g:ResourceTag/<tag-key>	-
			-	iam:PolicyURN	
iam:groups:attachPolicyV5	Grants permission to attach an identity policy to a group.	Permission_management	group *	-	-
			-	iam:PolicyURN	
iam:users:attachPolicyV5	Grants permission to attach an identity policy to an IAM user.	Permission_management	user *	g:ResourceTag/<tag-key>	-
			-	iam:PolicyURN	
iam:agencies:detachPolicyV5	Grants permission to detach an identity policy from an agency or a trust agency.	Permission_management	agency *	g:ResourceTag/<tag-key>	-
			-	iam:PolicyURN	

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:groups:detachPolicyV5	Grants permission to detach an identity policy from a group.	Permission_management	group *	-	-
			-	iam:PolicyURN	
iam:users:detachPolicyV5	Grants permission to detach an identity policy from an IAM user.	Permission_management	user *	g:ResourceTag/<tag-key>	-
			-	iam:PolicyURN	
iam:policies:listEntitiesV5	Grants permission to list attached entities for an identity policy.	List	policy *	-	-
iam:agencies:listAttachedPoliciesV5	Grants permission to list attached identity policies for an agency or a trust agency.	List	agency *	g:ResourceTag/<tag-key>	-
iam:groups:listAttachedPoliciesV5	Grants permission to list attached identity policies for a group.	List	group *	-	-
iam:users:listAttachedPoliciesV5	Grants permission to list attached identity policies for an IAM user.	List	user *	g:ResourceTag/<tag-key>	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:agencies:createServiceLinkedAgencyV5	Grants permission to create a service linked agency that allows a cloud service to perform actions on your behalf.	Write	agency *	-	-
			-	iam:ServicePrincipal	
iam:agencies:deleteServiceLinkedAgencyV5	Grants permission to delete a service linked agency.	Write	agency *	g:ResourceTag/<tag-key>	-
			-	iam:ServicePrincipal	
iam:agencies:getServiceLinkedAgencyDeletionStatusV5	Grants permission to retrieve deletion status of a service linked agency.	Read	agency *	-	-
iam:agencies:listV5	Grants permission to list agencies and trust agencies.	List	agency *	-	-
iam:agencies:getV5	Grants permission to retrieve information about an agency or a trust agency.	Read	agency *	g:ResourceTag/<tag-key>	-
iam:agencies:createV5	Grants permission to create a trust agency.	Write	agency *	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam:agencies:updateV5	Grants permission to update a trust agency.	Write	agency *	g:ResourceTag/<tag-key>	-
iam:agencies:deleteV5	Grants permission to delete a trust agency.	Write	agency *	g:ResourceTag/<tag-key>	-
iam:agencies:updateTrustPolicyV5	Grants permission to update the trust policy of a trust agency.	Write	agency *	g:ResourceTag/<tag-key>	-
iam::listTagsForResourceV5	Grants permission to list tags for a resource.	List	agency	g:ResourceTag/<tag-key>	-
			user	g:ResourceTag/<tag-key>	
iam::tagForResourceV5	Grants permission to tag a resource.	Tagging	agency	g:ResourceTag/<tag-key>	-
			user	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
iam::untagForResourceV5	Grants permission to untag a resource.	Tagging	agency	g:ResourceTag/<tag-key>	-
			user	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
iam::getAccountSummaryV5	Grants permission to retrieve information about IAM entity usage and IAM quotas in the IAM account.	List	-	-	-
iam::getAsymmetricSignatureSwitchV5	Grants permission to query asymmetric signature switch status of security token.	Read	-	-	-
iam::setAsymmetricSignatureSwitchV5	Grants permission to set asymmetric signature switch status of security token.	Write	-	-	-

Each API of IAM usually supports one or more actions. **Table 6-3** lists the supported actions and dependencies.

Table 6-3 Actions and dependencies supported by IAM APIs

API	Action	Dependencies
GET /v3.0/OS-CREDENTIAL/credentials	iam::listAccessKeys	-
POST /v3.0/OS-CREDENTIAL/credentials	iam::createAccessKey	-
GET /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam::getAccessKey	-

API	Action	Dependencies
PUT /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam::updateAccessKey	-
DELETE /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam::deleteAccessKey	-
GET /v3.0/OS-QUOTA/domains/{domain_id}	iam:quotas:list	-
GET /v3.0/OS-QUOTA/projects/{project_id}	iam:quotas:listForProject	-
GET /v3/projects	iam:projects:list	-
POST /v3/projects	iam:projects:create	-
GET /v3/users/{user_id}/projects	iam:projects:listForUser	-
PATCH /v3/projects/{project_id}	iam:projects:update	-
PUT /v3-ext/projects/{project_id}	iam:projects:update	-
GET /v3/groups	iam:groups:list	-
POST /v3/groups	iam:groups:create	-
GET /v3/groups/{group_id}	iam:groups:get	-
DELETE /v3/groups/{group_id}	iam:groups:delete	-
PATCH /v3/groups/{group_id}	iam:groups:update	-
GET /v3/groups/{group_id}/users	iam:groups:listUsers	-
HEAD /v3/groups/{group_id}/users/{user_id}	iam:groups:checkUser	-
PUT /v3/groups/{group_id}/users/{user_id}	iam:groups:addUser	-
DELETE /v3/groups/{group_id}/users/{user_id}	iam:groups:removeUser	-

API	Action	Dependencies
POST /v3.0/OS-USER/users	iam:users:create	-
GET /v3.0/OS-USER/users/{user_id}	iam:users:get	-
PUT /v3.0/OS-USER/users/{user_id}	iam:users:update	-
PUT /v3.0/OS-USER/users/{user_id}/info	iam:users:update	-
GET /v3/users	iam:users:list	-
POST /v3/users	iam:users:create	-
GET /v3/users/{user_id}	iam:users:get	-
DELETE /v3/users/{user_id}	iam:users:delete	-
PATCH /v3/users/{user_id}	iam:users:update	-
GET /v3/users/{user_id}/groups	iam:users:listGroups	-
GET /v3.0/OS-MFA/virtual-mfa-devices	iam:users:listVirtualMFADevices	-
POST /v3.0/OS-MFA/virtual-mfa-devices	iam:users:createVirtualMFADevice	-
DELETE /v3.0/OS-MFA/virtual-mfa-devices	iam:users:deleteVirtualMFADevice	-
GET /v3.0/OS-MFA/users/{user_id}/virtual-mfa-device	iam:users:getVirtualMFADevice	-
PUT /v3.0/OS-MFA/mfa-devices/bind	iam:users:bindVirtualMFADevice	-
PUT /v3.0/OS-MFA/mfa-devices/unbind	iam:users:unbindVirtualMFADevice	-
GET /v3.0/OS-USER/login-protects	iam:users:listLoginProtectSettings	-
GET /v3.0/OS-USER/users/{user_id}/login-protect	iam:users:getLoginProtectSetting	-
PUT /v3.0/OS-USER/users/{user_id}/login-protect	iam:users:updateLoginProtectSetting	-

API	Action	Dependencies
GET /v3/OS-FEDERATION/identity_providers	iam:identityProviders:list	-
GET /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:get	-
PUT /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:create	-
DELETE /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:delete	-
PATCH /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:update	-
GET /v3/OS-FEDERATION/mappings	iam:identityProviders:listMappings	-
GET /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:getMapping	-
PUT /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:createMapping	-
DELETE /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:deleteMapping	-
PATCH /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:updateMapping	-
GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols	iam:identityProviders:listProtocols	-
GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:getProtocol	-

API	Action	Dependencies
PUT /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:createProtocol	-
DELETE /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:deleteProtocol	-
PATCH /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:updateProtocol	-
GET /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata	iam:identityProviders:getSAMLMetadata	-
POST /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata	iam:identityProviders:createSAMLMetadata	-
GET /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config	iam:identityProviders:getOIDCConfig	-
POST /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config	iam:identityProviders:createOIDCConfig	-
PUT /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config	iam:identityProviders:updateOIDCConfig	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy	iam:securityPolicies:getProtectPolicy	-

API	Action	Dependencies
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy	iam:securityPolicies:updateProtectPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy	iam:securityPolicies:getPasswordPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy	iam:securityPolicies:updatePasswordPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy	iam:securityPolicies:getLoginPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy	iam:securityPolicies:updateLoginPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy	iam:securityPolicies:getConsoleAclPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy	iam:securityPolicies:updateConsoleAclPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy	iam:securityPolicies:getApiAclPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy	iam:securityPolicies:updateApiAclPolicy	-
GET /v3/roles	iam:roles:list	-
GET /v3/roles/{role_id}	iam:roles:get	-
GET /v3.0/OS-PERMISSION/role-assignments	iam::listRoleAssignments	-

API	Action	Dependencies
GET /v3/domains/{domain_id}/groups/{group_id}/roles	iam:groups:listRolesOnDomain	-
GET /v3/projects/{project_id}/groups/{group_id}/roles	iam:groups:listRolesOnProject	-
PUT /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:groups:grantRoleOnDomain	-
PUT /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:groups:grantRoleOnProject	-
HEAD /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:groups:checkRoleOnDomain	-
HEAD /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:groups:checkRoleOnProject	-
GET /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/inherited_to_projects	iam:groups:listRoles	-
HEAD /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects	iam:groups:checkRole	-
DELETE /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects	iam:groups:revokeRole	-
DELETE /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:groups:revokeRoleOnDomain	-
DELETE /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:groups:revokeRoleOnProject	-
PUT /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects	iam:groups:grantRole	-

API	Action	Dependencies
GET /v3.0/OS-ROLE/roles	iam:roles:list	-
GET /v3.0/OS-ROLE/roles/{role_id}	iam:roles:get	-
POST /v3.0/OS-ROLE/roles	iam:roles:create	-
POST /v3.0/OS-ROLE/roles	iam:roles:create	-
PATCH /v3.0/OS-ROLE/roles/{role_id}	iam:roles:update	-
PATCH /v3.0/OS-ROLE/roles/{role_id}	iam:roles:update	-
DELETE /v3.0/OS-ROLE/roles/{role_id}	iam:roles:delete	-
GET /v3.0/OS-AGENCY/agencies	iam:agencies:list	-
GET /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:get	-
POST /v3.0/OS-AGENCY/agencies	iam:agencies:create	-
PUT /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:update	-
DELETE /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:delete	-
GET /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles	iam:agencies:listRolesOnDomain	-
GET /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles	iam:agencies:listRolesOnProject	-
PUT /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:grantRoleOnDomain	-
PUT /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:grantRoleOnProject	-

API	Action	Dependencies
HEAD /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:checkRoleOnDomain	-
HEAD /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:checkRoleOnProject	-
DELETE /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:revokeRoleOnDomain	-
DELETE /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:revokeRoleOnProject	-
GET /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/inherited_to_projects	iam:agencies:listRoles	-
PUT /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:grantRole	-
HEAD /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:checkRole	-
DELETE /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:revokeRole	-
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups	iam::listGroupsAssignedEnterpriseProject	-

API	Action	Dependencies
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles	iam:groups:listRolesOnEnterpriseProject	-
PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}	iam:groups:grantRoleOnEnterpriseProject	-
DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}	iam:groups:revokeRoleOnEnterpriseProject	-
GET /v3.0/OS-PERMISSION/groups/{group_id}/enterprise-projects	iam:groups:listAssignedEnterpriseProjects	-
GET /v3.0/OS-PERMISSION/users/{user_id}/enterprise-projects	iam:users:listAssignedEnterpriseProjects	-
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users	iam::listUsersAssignedEnterpriseProject	-
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles	iam:users:listRolesOnEnterpriseProject	-
PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}	iam:users:grantRoleOnEnterpriseProject	-

API	Action	Dependencies
DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}	iam:users:revokeRoleOnEnterpriseProject	-
PUT /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments	iam:agencies:grantRoleOnEnterpriseProject	-
DELETE /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments	iam:agencies:revokeRoleOnEnterpriseProject	-
GET /v5/asymmetric-signature-switch	iam::getAsymmetricSignatureSwitchV5	-
PUT /v5/asymmetric-signature-switch	iam::setAsymmetricSignatureSwitchV5	-
GET /v5/mfa-devices	iam:mfa:listMFADevicesV5	-
POST /v5/virtual-mfa-devices	iam:mfa:createVirtualMFADeviceV5	-
DELETE /v5/virtual-mfa-devices	iam:mfa:deleteVirtualMFADeviceV5	-
POST /v5/mfa-devices/enable	iam:mfa:enableV5	-
POST /v5/mfa-devices/disable	iam:mfa:disableV5	-
GET /v5/password-policy	iam:securitypolicies:getPasswordPolicyV5	-
PUT /v5/password-policy	iam:securitypolicies:updatePasswordPolicyV5	-
GET /v5/login-policy	iam:securitypolicies:getLoginPolicyV5	-
PUT /v5/login-policy	iam:securitypolicies:updateLoginPolicyV5	-
GET /v5/users/{user_id}/access-keys	iam:credentials:listCredentialsV5	-

API	Action	Dependencies
GET /v5/users/{user_id}/access-keys/{access_key_id}/last-used	iam:credentials:showAccessKeyLastUsedV5	-
POST /v5/users/{user_id}/access-keys	iam:credentials:createCredentialV5	-
PUT /v5/users/{user_id}/access-keys/{access_key_id}	iam:credentials:updateCredentialV5	-
DELETE /v5/users/{user_id}/access-keys/{access_key_id}	iam:credentials:deleteCredentialV5	-
POST /v5/caller-password	iam:users:changePasswordV5	-
GET /v5/users/{user_id}/login-profile	iam:users:showLoginProfileV5	-
POST /v5/users/{user_id}/login-profile	iam:users:createLoginProfileV5	-
PUT /v5/users/{user_id}/login-profile	iam:users:updateLoginProfileV5	-
DELETE /v5/users/{user_id}/login-profile	iam:users:deleteLoginProfileV5	-
GET /v5/users	iam:users:listUsersV5	-
GET /v5/users/{user_id}	iam:users:getUserV5	-
GET /v5/users/{user_id}/last-login	iam:users:showUserLastLoginV5	-
POST /v5/users	iam:users:createUserV5	-
PUT /v5/users/{user_id}	iam:users:updateUserV5	-
DELETE /v5/users/{user_id}	iam:users:deleteUserV5	-
GET /v5/groups	iam:groups:listGroupsV5	-
GET /v5/groups/{group_id}	iam:groups:getGroupV5	-
POST /v5/groups	iam:groups:createGroupV5	-
PUT /v5/groups/{group_id}	iam:groups:updateGroupV5	-

API	Action	Dependencies
DELETE /v5/groups/{group_id}	iam:groups:deleteGroupV5	-
POST /v5/groups/{group_id}/add-user	iam:permissions:addUserToGroupV5	-
POST /v5/groups/{group_id}/remove-user	iam:permissions:removeUserFromGroupV5	-
GET /v5/policies	iam:policies:listV5	-
GET /v5/policies/{policy_id}	iam:policies:getV5	-
POST /v5/policies	iam:policies:createV5	-
DELETE /v5/policies/{policy_id}	iam:policies:deleteV5	-
GET /v5/policies/{policy_id}/versions	iam:policies:listVersionsV5	-
GET /v5/policies/{policy_id}/versions/{version_id}	iam:policies:getVersionV5	-
POST /v5/policies/{policy_id}/versions	iam:policies:createVersionV5	-
DELETE /v5/policies/{policy_id}/versions/{version_id}	iam:policies:deleteVersionV5	-
POST /v5/policies/{policy_id}/versions/{version_id}/set-default	iam:policies:setDefaultVersionV5	-
POST /v5/policies/{policy_id}/attach-agency	iam:agencies:attachPolicyV5	-
POST /v5/policies/{policy_id}/attach-group	iam:groups:attachPolicyV5	-
POST /v5/policies/{policy_id}/attach-user	iam:users:attachPolicyV5	-
POST /v5/policies/{policy_id}/detach-agency	iam:agencies:detachPolicyV5	-
POST /v5/policies/{policy_id}/detach-group	iam:groups:detachPolicyV5	-

API	Action	Dependencies
POST /v5/policies/{policy_id}/detach-user	iam:users:detachPolicyV5	-
GET /v5/policies/{policy_id}/attached-entities	iam:policies:listEntitiesV5	-
GET /v5/agencies/{agency_id}/attached-policies	iam:agencies:listAttachedPoliciesV5	-
GET /v5/groups/{group_id}/attached-policies	iam:groups:listAttachedPoliciesV5	-
GET /v5/users/{user_id}/attached-policies	iam:users:listAttachedPoliciesV5	-
PUT /v5/service-linked-agencies	iam:agencies:createServiceLinkedAgencyV5	-
DELETE /v5/service-linked-agencies/{agency_id}	iam:agencies:deleteServiceLinkedAgencyV5	-
GET /v5/service-linked-agencies/deletion-task/{deletion_task_id}	iam:agencies:getServiceLinkedAgencyDeletionStatusV5	-
GET /v5/agencies	iam:agencies:listV5	-
GET /v5/agencies/{agency_id}	iam:agencies:getV5	-
POST /v5/agencies	iam:agencies:createV5	-
PUT /v5/agencies/{agency_id}	iam:agencies:updateV5	-
DELETE /v5/agencies/{agency_id}	iam:agencies:deleteV5	-
PUT /v5/agencies/{agency_id}/trust-policy	iam:agencies:updateTrustPolicyV5	-
GET /v5/{resource_type}/{resource_id}/tags	iam::listTagsForResourceV5	-
POST /v5/{resource_type}/{resource_id}/tags/create	iam::tagForResourceV5	-

API	Action	Dependencies
DELETE /v5/{resource_type}/{resource_id}/tags/delete	iam::untagForResourceV5	-
GET /v5/account-summary	iam::getAccountSummaryV5	-

Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in Table 6-4, the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for IAM.

Table 6-4 Resource types supported by IAM

Resource Type	URN
agency	iam::<account-id>:agency:<agency-name-with-path>
policy	iam::<account-id>:policy:<policy-name-with-path>
user	iam::<account-id>:user:<user-name>
mfa	iam::<account-id>:mfa:<mfa-name>
group	iam::<account-id>:group:<group-name>

Conditions

Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see **Global Condition Keys**.

  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, iam) apply only to operations of the xx service. For details, see **Table 6-5**.
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see **operators**.

Service-specific condition keys supported by IAM

The following table lists the condition keys that you can define in identity policies for IAM. You can include these condition keys to specify conditions for when your identity policy is in effect.

Table 6-5 Service-specific condition keys supported by IAM

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
iam:PolicyURN	string	Single-valued	Filters access by the URN of an identity policy.
iam:ServicePrincipal	string	Single-valued	Filters access by the service principal of the cloud service to which this service linked agency is passed.

6.3 STS Identity Policy-based Authorization Reference

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the **Organizations** service also provides **Service Control Policies (SCPs)** to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are

available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see **How IAM Is Different from Organizations for Access Control?**.

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see **Creating a Custom Identity Policy**.
- For details about how to use these elements to edit a custom SCP, see **Creating an SCP**.

Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

  For details about the resource types defined by STS, see **Resources**.
- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

  For details about the condition keys defined by STS, see **Conditions**.
- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see **Policies and Identity Policies**.

The following table lists the actions that you can define in identity policy statements for STS.

Table 6-6 Actions supported by STS

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
sts:agencies:assume	Grants permission to obtain a set of temporary credentials that you can use to access resources that you might not normally have access to.	Write	agency *	g:ResourceTag/<tag-key>	-
			-	• sts:ExternalId • sts:SourceIdentity • sts:TransitiveTagKeys • sts:AgencySessionName • g:RequestTag/<tag-key> • g:TagKeys • g:SourceAccount • g:SourceUrn	
sts::decodeAuthorizationMessage	Grants permission to decode additional information about the authorization status of a request from an encoded message returned in response to a request.	Write	-	-	-
sts::setSourceIdentity	Grants permission to set a source identity on a STS session.	Write	agency *	g:ResourceTag/<tag-key>	-
			-	sts:SourceIdentity	

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
sts::tagSession	Grants permission to add tags to a STS session.	Tagging	agency *	g:ResourceTag/<tag-key>	-
			-	• sts:TransitiveTagKeys • g:RequestTag/<tag-key> • g:TagKeys	
sts::createServiceBearerToken	Grants permission to get the service bearer token.	Write	-	• sts:DurationTime • sts:ServiceName	-

Each API of STS usually supports one or more actions. **Table 6-7** lists the supported actions and dependencies.

Table 6-7 Actions and dependencies supported by STS APIs

API	Action	Dependencies
POST /v5/agencies/assume	sts:agencies:assume	• sts::tagSession • sts::setSourceIdentity
POST /v5/decode-authorization-message	sts::decodeAuthorization-Message	-

Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in **Table 6-8**, the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for STS.

Table 6-8 Resource types supported by STS

Resource Type	URN
agency	iam::<account-id>:agency:<agency-name-with-path>
assumed-agency	sts::<account-id>:assumed-agency:<agency-name>/<session-name>

Conditions

Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see **Global Condition Keys**.
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, sts) apply only to operations of the xx service. For details, see **Table 6-9**.
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see **operators**.

Service-specific condition keys supported by STS

The following table lists the condition keys that you can define in identity policies for STS. You can include these condition keys to specify conditions for when your identity policy is in effect.

Table 6-9 Service-specific condition keys supported by STS

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
sts:ExternalId	string	Single-valued	Filters access by the external ID that is passed in the request.
sts:SourceIdentity	string	Single-valued	Filters access by the source identity that is passed in the request.
sts:TransitiveTagKeys	string	Multivalued	Filters access by the transitive tag keys that are passed in the request.
sts:AgencySessionName	string	Single-valued	Filters access by the agency session name required when you assume an agency.
sts:DurationTime	numeric	Single-valued	Filters access by the duration times when you create a bearer token.
sts:ServiceName	string	Single-valued	Filters access by the service name when you create a bearer token.

6.4 IAM Access Analyzer Identity Policy-based Authorization Reference

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the **Organizations** service also provides **Service Control Policies (SCPs)** to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see **How IAM Is Different from Organizations for Access Control?**.

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see **Creating a Custom Identity Policy**.
- For details about how to use these elements to edit a custom SCP, see **Creating an SCP**.

Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

  For details about the resource types defined by IAM Access Analyzer, see **Resources**.
- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

  For details about the condition keys defined by IAM Access Analyzer, see **Conditions**.
- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see **Policies and Identity Policies**.

The following table lists the actions that you can define in identity policy statements for IAM Access Analyzer.

Table 6-10 Actions supported by IAM Access Analyzer

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
AccessAnalyzer:analyzer:create	Grants permission to create an access analyzer.	Write	analyzer *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
AccessAnalyzer:analyzer:get	Grants permission to retrieve the access analyzer information.	Read	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:list	Grants permission to retrieve the access analyzer list.	List	analyzer *	-	-
AccessAnalyzer:analyzer:delete	Grants permission to delete an access analyzer.	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:update	Grants permission to update the specified access analyzer.	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:scan	Grants permission to start a scan for the specified access analyzer.	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:getFinding	Grants permission to retrieve findings.	Read	analyzer *	g:ResourceTag/<tag-key>	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
AccessAnalyzer:analyzer:listFindings	Grants permission to retrieve the finding list.	List	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:updateFindings	Grants permission to update the findings.	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer::tagResource	Grants permission to add a tag to a resource.	Tagging	analyzer *	g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
AccessAnalyzer::untagResource	Grants permission to remove a tag from a resource.	Tagging	analyzer *	g:ResourceTag/<tag-key>	-
			-	g:TagKeys	
AccessAnalyzer:archiveRule:create	Grants permission to create an archive rule for the specified access analyzer.	Write	archiveRule *	-	-
AccessAnalyzer:archiveRule:get	Grants permission to retrieve the archive rule for the specified access analyzer.	Read	archiveRule *	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
AccessAnalyzer:archiveRule:list	Grants permission to retrieve the archive rule list for the specified access analyzer.	List	archiveRule *	-	-
AccessAnalyzer:archiveRule:update	Grants permission to modify the archive rule for the specified access analyzer.	Write	archiveRule *	-	-
AccessAnalyzer:archiveRule:delete	Grants permission to delete the archive rule for the specified access analyzer.	Write	archiveRule *	-	-
AccessAnalyzer:archiveRule:apply	Grants permission to apply an archive rule.	Write	archiveRule *	-	-
AccessAnalyzer:analyzer:createPreview	Grants permission to create an access preview for the specified access analyzer.	Write	analyzer *	g:ResourceTag/<tag-key>	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
AccessAnalyzer:analyzer:getPreview	Grants permission to retrieve the access preview information for the specified access analyzer.	Read	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:listPreviews	Grants permission to retrieve the access preview list for the specified access analyzer.	List	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:listPreviewFindings	Grants permission to retrieve the preview finding list for the specified access analyzer.	List	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:createResourceConfigurations	Grants permission to create or update resource configurations.	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:listResourceConfigurations	Grants permission to retrieve the list for resource configurations.	List	analyzer *	g:ResourceTag/<tag-key>	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
AccessAnalyzer:analyzer:deleteResourceConfigurations	Grants permission to delete the resource configurations.	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer::validatePolicy	Grants permission to validate a policy.	Read	-	-	-
AccessAnalyzer::checkNoNewAccess	Grants permission to check whether the updated policy has new access permissions.	Read	-	-	-
AccessAnalyzer:notificationSetting:list	Grants permission to retrieve the notification setting list.	Read	notificationSetting *	-	-
AccessAnalyzer:notificationSetting:create	Grants permission to create a notification setting.	Write	notificationSetting *	-	-
AccessAnalyzer:notificationSetting:get	Grants permission to retrieve the notification setting.	Read	notificationSetting *	-	-
AccessAnalyzer:notificationSetting:update	Grants permission to modify the notification setting.	Write	notificationSetting *	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
AccessAnalyzer:notificationSetting:delete	Grants permission to delete the notification setting.	Write	notificationSetting *	-	-

Each API of IAM Access Analyzer usually supports one or more actions. **Table 6-11** lists the supported actions and dependencies.

Table 6-11 Actions and dependencies supported by IAM Access Analyzer APIs

API	Action	Dependencies
POST /v5/analyzers	AccessAnalyzer:analyzer:create	iam:agencies:createServiceLinkedAgencyV5
GET /v5/analyzers/{analyzer_id}	AccessAnalyzer:analyzer:get	-
GET /v5/analyzers	AccessAnalyzer:analyzer:list	-
DELETE /v5/analyzers/{analyzer_id}	AccessAnalyzer:analyzer:delete	-
PUT /v5/analyzers/{analyzer_id}	AccessAnalyzer:analyzer:update	-
POST /v5/analyzers/{analyzer_id}/scan	AccessAnalyzer:analyzer:scan	-
GET /v5/analyzers/{analyzer_id}/findings/{finding_id}	AccessAnalyzer:analyzer:getFinding	-
POST /v5/analyzers/{analyzer_id}/findings	AccessAnalyzer:analyzer:listFindings	-
PUT /v5/analyzers/{analyzer_id}/findings	AccessAnalyzer:analyzer:updateFindings	-

API	Action	Dependencies
POST /v5/{resource_type}/{resource_id}/tags/create	AccessAnalyzer::tagResource	-
POST /v5/{resource_type}/{resource_id}/tags/delete	AccessAnalyzer::untagResource	-
POST /v5/analyzers/{analyzer_id}/archive-rules	AccessAnalyzer:archiveRule:create	-
GET /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}	AccessAnalyzer:archiveRule:get	-
GET /v5/analyzers/{analyzer_id}/archive-rules	AccessAnalyzer:archiveRule:list	-
PUT /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}	AccessAnalyzer:archiveRule:update	-
DELETE /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}	AccessAnalyzer:archiveRule:delete	-
POST /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}/apply	AccessAnalyzer:archiveRule:apply	-
POST /v5/analyzers/{analyzer_id}/access-previews	AccessAnalyzer:analyzer:createPreview	-
GET /v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}	AccessAnalyzer:analyzer:getPreview	-

API	Action	Dependencies
GET /v5/analyzers/{analyzer_id}/access-previews	AccessAnalyzer:analyzer:listPreviews	-
POST /v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}/findings	AccessAnalyzer:analyzer:listPreviewFindings	-
POST /v5/analyzers/{analyzer_id}/resource-configurations/create	AccessAnalyzer:analyzer:createResourceConfigurations	-
GET /v5/analyzers/{analyzer_id}/resource-configurations	AccessAnalyzer:analyzer:listResourceConfigurations	-
POST /v5/analyzers/{analyzer_id}/resource-configurations/delete	AccessAnalyzer:analyzer:deleteResourceConfigurations	-
POST /v5/policies/validate	AccessAnalyzer::validatePolicy	-
POST /v5/policies/check-no-new-access	AccessAnalyzer::checkNoNewAccess	-
GET /v5/notification-settings	AccessAnalyzer:notificationSetting:list	-
POST /v5/notification-settings	AccessAnalyzer:notificationSetting:create	-
GET /v5/notification-settings/{notification_setting_id}	AccessAnalyzer:notificationSetting:get	-

API	Action	Dependencies
PUT /v5/notification-settings/{notification_setting_id}	AccessAnalyzer:notificationSetting:update	-
DELETE /v5/notification-settings/{notification_setting_id}	AccessAnalyzer:notificationSetting:delete	-

Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in Table 6-12, the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for IAM Access Analyzer.

Table 6-12 Resource types supported by IAM Access Analyzer

Resource Type	URN
analyzer	AccessAnalyzer:<region>:<account-id>:analyzer:<analyzer-id>
notificationSetting	AccessAnalyzer:<region>:<account-id>:notificationSetting:<notification-setting-id>
archiveRule	AccessAnalyzer:<region>:<account-id>:archiveRule:<analyzer-id>/<archive-rule-id>

Conditions

IAM Access Analyzer does not support service-specific condition keys in identity policies.It can only use global condition keys applicable to all services. For details, see Global Condition Keys.

7 Appendix

7.1 Status Codes

Table 7-1 Status codes

Status Code	Message Title	Description
100	Continue	The client should continue with its request. This interim response is used to inform the client that the initial part of the request has been received and has not yet been rejected by the server.
101	Switching Protocols	The requester has asked the server to switch protocols and the server has agreed to do so. The protocol should be switched only when it is advantageous to do so. For example, switching to a newer version of HTTP is advantageous over older versions.
201	Created	The request has been fulfilled and resulted in a new resource being created.
202	Accepted	The request has been accepted for processing, but the processing has not been completed.
203	Non-Authoritative Information	The server successfully processed the request, but is returning information that may be from another source.
204	NoContent	The server has successfully processed the request, but is not returning any response body. The status code is returned in response to an HTTP **OPTIONS** request.

Status Code	Message Title	Description
205	Reset Content	The server successfully processed the request, but is not returning any content.
206	Partial Content	The server has fulfilled the partial **GET** request for the resource.
300	Multiple Choices	There are multiple options for the resource from which the client may choose. For example, this code could be used to present a list of resource characteristics and addresses from which the client such as a browser may choose.
301	Moved Permanently	The requested resource has been assigned a new permanent URI and any future references to this resource should use one of the returned URIs.
302	Found	The requested resource resides temporarily under a different URI.
303	See Other	The response to the request can be found under a different URI and should be retrieved using a **GET** or **POST** method.
304	Not Modified	The requested resource has not been modified. When the server returns this status code, it does not return any resources.
305	Use Proxy	The requested resource must be accessed through a proxy.
306	Unused	This HTTP status code is no longer used.
400	BadRequest	The request could not be understood by the server due to malformed syntax. The client should not repeat the request without modifications.
401	Unauthorized	The authorization information provided by the client is incorrect or invalid.
402	Payment Required	This status code is reserved for future use.
403	Forbidden	The server understood the request, but is refusing to fulfill it. The server has received the request and understood it, but the server is refusing to respond to it. The client should not repeat the request without modifications.

Status Code	Message Title	Description
404	NotFound	The requested resource cannot be found. The client should not repeat the request without modifications.
405	MethodNotAllowed	The method specified in the request is not allowed for the requested resource. The client should not repeat the request without modifications.
406	Not Acceptable	The server cannot fulfill the request based on the content characteristics of the request.
407	Proxy Authentication Required	This code is similar to 401, but indicates that the client must first authenticate itself with the proxy.
408	Request Time-out	The client does not produce a request within the time that the server was prepared to wait. The client may repeat the request without modifications at any later time.
409	Conflict	The request could not be completed due to a conflict with the current state of the resource. This status code indicates that the resource that the client attempts to create already exists, or the request fails to be processed because of the update of the conflict request.
410	Gone	The requested resource is no longer available. The requested resource has been deleted permanently.
411	Length Required	The server refuses to process the request without a defined **Content-Length**.
412	Precondition Failed	The server does not meet one of the preconditions that the requester puts on the request.
413	Request Entity Too Large	The server is refusing to process a request because the request entity is larger than the server is willing or able to process. The server may close the connection to prevent the client from continuing the request. If the condition is temporary, the server should include a **Retry-After** header field to indicate that it is temporary and after what time the client may try again.

Status Code	Message Title	Description
414	Request-URI Too Large	The server is refusing to service the request because the request URI is longer than the server is willing to interpret.
415	Unsupported Media Type	The server is refusing to service the request because the entity of the request is in a format not supported by the requested resource for the requested method.
416	Requested range not satisfiable	The requested range is invalid.
417	Expectation Failed	The server fails to meet the requirements of the **Expect** request header field.
422	UnprocessableEntity	The request was well-formed but was unable to be followed due to semantic errors.
429	TooManyRequests	The client has sent more requests than its rate limit is allowed within a given amount of time, or the server has received more requests than it is able to process within a given amount of time. In this case, the client should repeat requests after the time specified in the **Retry-After** header of the response expires.
500	InternalServerError	The server encountered an unexpected condition which prevented it from fulfilling the request.
501	Not Implemented	The server does not support the functionality required to fulfill the request.
502	Bad Gateway	The server, while acting as a gateway or proxy, received an invalid response from the upstream server it accessed in attempting to fulfill the request.
503	ServiceUnavailable	The requested service is unavailable. The client should not repeat the request without modifications.
504	ServerTimeout	The request cannot be fulfilled within a given amount of time. The response will reach the client only if the request carries a **timeout** parameter.
505	HTTP Version not supported	The server does not support the HTTP protocol version used in the request.

7.2 Error Codes

If an API fails to be called, an error code, instead of the service data, is returned. The returned error code can be used to identify the failure cause. In the HTTP protocol, a 4*xx* or 5*xx* response will be returned when an error occurs. The response contains the specific error code and information. If you are unable to identify the cause of an error, contact customer service and provide the error code so that we can help you solve the problem as soon as possible.

Error Response Body Format

If an error occurs during API calling, an error code and a message will be displayed. The following shows an error response body.

```
{
   "error_msg": "attached policies per agency limit exceeded",
   "error_code": "PAP5.0003",
   "request_id": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
}
```

In the response body, **error_code** is an error code, **error_msg** provides information about the error, and **request_id** indicates the request ID.

In particular, if an error occurs due to lack of permissions, the error response body is as follows:

```
{
   "error_msg": "access denied: xxx...xxx",
   "error_code": "PAP5.0001",
   "request_id": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
   "encoded_authorization_message": "xxx...xxx"
}
```

In the response body, **encoded_authorization_message** is an additional field provided in this scenario, and indicates the encrypted authentication failure information. It can be decrypted using the STS5 decryption API.

Error Code Description

Table 7-2 Error codes

Status Code	Error Code	Error Message	Description	Measure
400	PAP5.0010	invalid marker	Invalid marker.	Check the value of the **marker** field.
400	PAP5.0011	malformed policy document	Incorrect identity policy or trust policy.	Check the value of the **policy document** field.

Status Code	Error Code	Error Message	Description	Measure
400	PAP5.0029	invalid agency name	Invalid trust agency name.	Check the value of the **agency name** field.
400	PAP5.0030	invalid path	Invalid path.	Check the value of the **path** field.
400	PAP5.0033	duplicate key	Duplicate key value.	Check the request or contact technical support.
400	PAP5.0036	tag non-compliant	The tag value conflicts with preset tag policies.	Check the request or contact technical support.
400	PAP5.0038	This operation is only supported by v5 agencies	This operation is only supported by trust agencies.	Check the request or contact technical support.
400	PAP5.0040	invalid caller	Invalid caller.	Check whether the caller is the IAM user.
400	PAP5.0041	invalid serial number	Invalid serial number.	Check the value of the **serial number** field.
400	PAP5.0046	missing header `x-user-profile`	The **x-user-profile** is missing in the request header.	Check the request or contact technical support.
403	PAP5.0001	access denied: %s	Access denied.	Check whether this operation is allowed.
404	PAP5.0012	no such agency	Agency or trust agency not found.	Check the request or contact technical support.
404	PAP5.0014	no such authorization schema	Authorization summary not found.	Check the request or contact technical support.
404	PAP5.0015	no such deletion task	Deletion task not found.	Check the request or contact technical support.
404	PAP5.0016	no such group	User group not found.	Check the request or contact technical support.

Status Code	Error Code	Error Message	Description	Measure
404	PAP5.0018	no such policy	Identity policy not found.	Check the request or contact technical support.
404	PAP5.0019	no such policy attachment	Identity policy attachment record not found.	Check the request or contact technical support.
404	PAP5.0020	no such policy version	Identity policy version not found.	Check the request or contact technical support.
404	PAP5.0021	no such user	IAM user not found.	Check the request or contact technical support.
404	PAP5.0022	no such service linked agency	Service-linked agency not found.	Check the request or contact technical support.
404	PAP5.0023	no such service principal	Service principal not found.	Check the request or contact technical support.
404	PAP5.0034	no such domain	Tenant not found.	Check the request or contact technical support.
404	PAP5.0037	Resource tag not found	Resource tag not found.	Check the request or contact technical support.
409	PAP5.0003	attached policies per agency limit exceeded	Maximum identity policy attachments reached for a single agency or trust agency.	Detach unnecessary identity policies from the agency or trust agency.
409	PAP5.0004	attached policies per group limit exceeded	Maximum identity policy attachments reached for a user group.	Detach unnecessary identity policies from the user group.
409	PAP5.0005	attached policies per user limit exceeded	Maximum identity policy attachments reached for an IAM user.	Detach unnecessary identity policies from the IAM user.

Status Code	Error Code	Error Message	Description	Measure
409	PAP5.0006	concurrent modification	Concurrent modifications.	Try again later.
409	PAP5.0007	delete conflict: %s	Conflict exists and deletion failed.	Resolve the conflict.
409	PAP5.0024	policies limit exceeded	Maximum custom identity policies reached.	Delete unnecessary custom identity policies.
409	PAP5.0025	policy already exists	Identity policy already exists.	Check the request or contact technical support.
409	PAP5.0026	policy attachment already exists	Identity policy already attached.	Check the request or contact technical support.
409	PAP5.0027	policy size limit exceeded	Maximum number of bytes %*d* of an identity policy or trust policy reached (excluding blank characters).	Simplify the identity policy or trust policy.
409	PAP5.0028	versions per policy limit exceeded	Maximum versions reached for an identity policy.	Delete unnecessary identity policy versions.
409	PAP5.0031	agency already exists	The agency or trust agency already exists.	Check the request or contact technical support.
409	PAP5.0035	tags limit exceeded	Maximum tags reached.	Check the request or contact technical support.
409	PAP5.0039	mfa device already exists	The virtual MFA device already exists.	Check the request or contact technical support.
409	PAP5.0042	user already exists	The IAM user already exists.	Check the request or contact technical support.
409	PAP5.0043	group already exists	The user group already exists.	Check the request or contact technical support.

Status Code	Error Code	Error Message	Description	Measure
409	PAP5.0044	user already in group	The IAM user already exists in the user group.	Check the request.
409	PAP5.0045	login profile already exists	The login information already exists.	Check the request or contact technical support.

