IAM Identity Center

API Reference

Issue 01

Date 2025-08-21

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

IAM Identity Center helps you centrally manage your workforce identities and their access to multiple accounts through Huawei Cloud Organizations. You can create identities for your entire enterprise at one go and give them single sign-on (SSO) access with managed permissions. The IAM Identity Center administrator creates users, assigns passwords, and manages users by group. A single portal provides users with password-based SSO access to multiple accounts. A user who has passed the security verification in an application can access protected resources in other applications without logging in again.

Endpoints

An endpoint is the request address for calling an API. Endpoints vary depending on services and regions. For the endpoints of all services, see **Regions and Endpoints**.

Concepts

- Account

  An account is created upon successful registration. 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, which should not be used directly to perform routine management. For security purposes, create Identity and Access Management (IAM) users and grant them permissions for routine management.

- User

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

  API authentication requires information such as the account name, username, and password.

- 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.

For details, see **Region and AZ**.

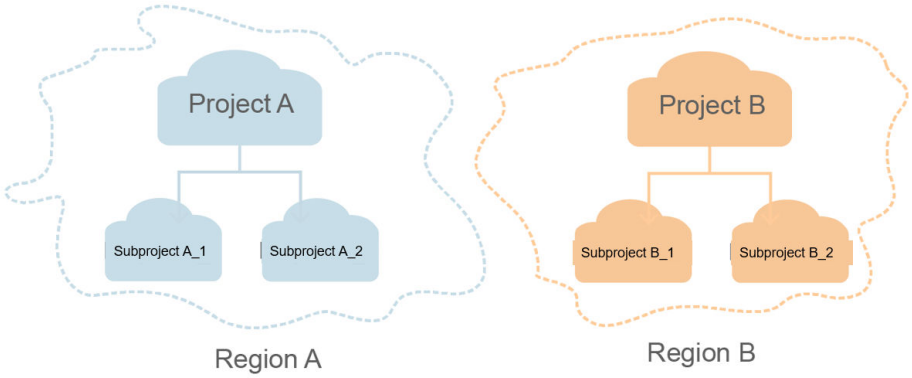
- AZ

  An availability zone (AZ) comprises one or more physical data centers equipped with independent ventilation, fire, water, and electricity facilities. Compute, network, storage, and other resources in an AZ are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

- Project

  A project corresponds to a region. Default projects are defined to group and physically isolate resources (including compute, storage, and network resources) across regions. Users can be granted permissions in a default project to access all resources under their accounts in the region associated with the project. If you need more refined access control, create subprojects under a default project and purchase resources in subprojects. Then you can assign users the permissions required to access only the resources in the specific subprojects.

Figure 1-1 Project isolating model



2 API Overview

Table 2-1 IAM APIs

Type	Description
4.1 Instance Management	List instances.
4.2 Access Control Attribute Management	Enable, obtain, update, and disable access control attributes for a specified instance.
4.3 Permission Set Management	Add, delete, modify, and query permission sets; attach, detach, and list system-defined identity policies or policies; query, attach, or delete custom identity policies or policies of a permission set; attach permission sets to an account; query the attachment status of a permission set; list accounts associated with a permission set; and list permission sets provisioned to an account.
4.4 Account Assignment Management	Add, delete, and query account assignments; query creation and deletion statuses of account assignments.
4.5 Tag Management	List, add, and remove tags for a specified permission set.
4.11 User Management	Add, delete, modify, and query users; query user IDs.
4.12 Group Management	Add, delete, modify, and query groups; query group IDs.
4.13 Group Membership Management	Add, delete, and query group membership; query the membership ID; list users in a group, list groups to which a user is added; query whether a user is a member of a group.
4.18 SCIM User Management	Add, modify, and delete users based on the SCIM protocol.

Type	Description
4.19 SCIM Group Management	Add, modify, and delete groups based on the SCIM protocol.
4.20 Service Provider (SP) Management	Query the SCIM configuration in the service provider (SP).
4.21 Client Management	Register a client.
4.22 Token Management	Create a token.
4.23 Device Authorization Management	Request device authorization.
4.24 Authorization Management	Log out of a user.
4.25 Account Management	List account information.
4.26 Agency Management	List account agencies or trust agencies.
4.27 Credentials Management	Obtain credentials for agencies or trust agencies.

3 Calling APIs

3.1 Making an API Request

This section describes the structure of a REST API request and use the API for listing instances as an example to describe how to call an API.

Request URI

A request URI is in the following format:

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

Table 3-1 Request URL

Parameter	Description
URI-scheme	Protocol used to transmit requests. All APIs use HTTPS.
Endpoint	Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints**. For example, the endpoint of IAM Identity Center is **identitycenter.myhuaweicloud.com**.
resource-path	Access path of an API for performing the specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API for **listing instances** is **/v1/instances**.
query-string	An optional query parameter. 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 queried.

For example, to list instances in IAM Identity Center, obtain the endpoint of IAM Identity Center (identitycenter.myhuaweicloud.com) and find **resource-path (/v1/instances)** in the URI of the API for **4.1.1 Listing Instances**. Then, construct the URI as follows:


```
https://identitycenter.myhuaweicloud.com/v1/instances
```

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** value 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 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 used to list instances, the request method is **GET**. The request is as follows:

```
GET https://identitycenter.myhuaweicloud.com/v1/instances
```

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 headers are as follows:

- **Content-Type** (mandatory): specifies the type or format of the message body. The default value is **application/json**.
- **Authorization** (mandatory): specifies the signature information contained in the request. For details about AK/SK authentication, see **AK/SK Authentication**.
- **X-Sdk-Date** (mandatory): specifies the time when the request was sent, for example, **20221107T020014Z**.
- **Host** (mandatory): specifies the host address, for example, **identitycenter.myhuaweicloud.com**.

  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 details about AK/SK authentication, see **AK/SK Authentication**.

For the API in **4.1.1 Listing Instances**, the request is as follows:

```
GET https://identitycenter.myhuaweicloud.com/v1/instances
content-type: application/json
X-Sdk-Date: 20230330T021902Z
```



```
host: identitycenter.myhuaweicloud.com
Authorization: SDK-HMAC-SHA256 Access=xxxxxxxxxxxxxxxxxxx, SignedHeaders=content-type;host;x-sdk-date, Signature=xxxxxxxxxxxxxxxxxxxx
```

(Optional) 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.

The request body varies between APIs. Some APIs do not require the request body, such as the APIs requested using the **GET** and **DELETE** methods.

3.2 Authentication

AK/SK authentication is used for calling APIs. Specifically, requests are encrypted using the access key (AK) or secret access key (SK) to provide higher security.

AK/SK Authentication

NOTE

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

In AK/SK authentication, AK/SK is used to sign a request and the signature is then added to the request 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 authentication, you can use an AK/SK to sign requests based on the signature algorithm or use the signing SDK to sign requests. For details about how to sign requests and use the signing SDK, see **AK/SK Signing and Authentication Guide**.

NOTICE

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

3.3 Response

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

Status Codes

A status code is a group of digits, ranging from 1xx to 5xx. It indicates the status of a request. For more information, see **5.1 Status Codes**.

For example, if status code **200** is returned for calling the API used to list instances, the request is successful.

Response Header

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

The following table describes common response headers.

Table 3-2 Common response headers

Header	Description
Content-Type	Type of the resource content. Type: string Default value: none
Connection	Whether the connection to the server is a long connection or a short connection. Type: string Valid values: keep-alive | close Default value: none
Date	Date when the server responded to the request. Type: string Default value: none
X-Request-Id	Uniquely identifies the request. The value is generated by the service and can be used for troubleshooting. Type: string Default value: none

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.

For the API in **4.1.1 Listing Instances**, the following message body is returned:

```
{
   "instances": [
      {
         "identity_store_id": "d-66f****b80",
         "instance_id": "ins-2c1e********f3c6",
         "alias": null,
         "instance_urn": "IdentityCenter::system:instance:ins-2c1e********f3c6"
      }
   ],
   "page_info": {
      "next_marker": null,
      "current_count": 1
   }
}
```


If an error occurs during API calling, an error code and a message will be displayed. The following shows an error response body.

```
{
    "error_code": "IIC.1215",
    "error_msg": "only organizations administrator account can operate, please log in to the administrator account!",
    "request_id": "e311530**********51311"
}
```

In the response body, **error_code** is an error code. **error_msg** provides information about the error. **request_id** uniquely identifies the request and its value is generated by the service and can be used for troubleshooting.

4 API

4.1 Instance Management

4.1.1 Listing Instances

Function

This API is used to list IAM Identity Center instances. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances

Table 4-1 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**

Request Parameters

Table 4-2 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-3 Parameters in the response body

Parameter	Type	Description
instances	Array of objects	IAM Identity Center instance list.
page_info	Object	Pagination information.

Table 4-4 instances

Parameter	Type	Description
identity_store_id	String	Globally unique identifier (ID) of the identity source associated with an IAM Identity Center instance. Minimum length: **1** Maximum length: **64**
instance_id	String	Globally unique ID of an IAM Identity Center instance. Minimum length: **20** Maximum length: **20**
alias	String	User-defined alias for the identity source ID.
instance_urn	String	Uniform Resource Name (URN) of an instance.

Table 4-5 page_info

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**.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-6 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-7 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing the instance list of IAM Identity Center

```
GET https://{hostname}/v1/instances
```


Example Response

Status code: 200

Successful

```
{
  "instances" : [ {
    "identity_store_id" : "d-a00aaaa33f",
    "alias" : "new-store-id-123",
    "instance_id" : "ins-bd8baaaaaaade60"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.1.2 Querying the Region Where a Service Instance Is Enabled

Function

This API is used to query the region where an IAM Identity Center instance is enabled. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/registered-regions

Request Parameters

Table 4-8 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-9 Parameters in the response body

Parameter	Type	Description
regions	Array of **RegionDto** objects	Site list.

Table 4-10 RegionDto

Parameter	Type	Description
region_id	String	Region ID.

Status code: 400

Table 4-11 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-12 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-13 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Querying the region where an IAM Identity Center service instance is enabled

```
GET https://{hostname}/v1/registered-regions
```

Example Response

Status code: 200

Successful

```
{
  "regions" : [ {
    "region_id" : "cn-north-4"
  } ]
}
```

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.1.3 Obtaining Identity Source Configurations

Function

This API is used to obtain identity source configurations of an IAM Identity Center service instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/identity-store-associations

Table 4-14 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-15 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-16 Parameters in the response body

Parameter	Type	Description
identity_store_associations	Array of **IdentityStoreDto** objects	Configuration of the identity source associated with an IAM Identity Center service instance.

Table 4-17 IdentityStoreDto

Parameter	Type	Description
identity_store_id	String	Globally unique ID of the identity source associated with an IAM Identity Center instance.
identity_store_type	String	Identity source type.
authentication_type	String	Login authentication type.

Parameter	Type	Description
provisioning_type	Array of strings	Provisioning type.
status	String	Whether the identity source is enabled.

Status code: 400

Table 4-18 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-19 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-20 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Obtaining identity source configurations of an IAM Identity Center service instance


```
GET https://{hostname}/v1/instances/{instance_id}/identity-store-associations
```

Example Response

Status code: 200

Successful

```
{
  "identity_store_associations" : [ {
    "identity_store_id" : "d-xxxxx",
    "identity_store_type" : "UserPool",
    "authentication_type" : "SAML_2.0",
    "provisioning_type" : [ "DEFAULT" ],
    "status" : "ENABLED"
  } ]
}
```

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.1.4 Selecting a Region for Enabling a Service Instance

Function

This API is used to select a region where an IAM Identity Center service instance is to be enabled. It can be called only from the organization's management account.

URI

POST /v1/register-regions

Request Parameters

Table 4-21 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-22 Parameters in the request body

Parameter	Mandatory	Type	Description
region_id	Yes	String	Region ID.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-23 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-24 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 409

Table 4-25 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Selecting a region where an IAM Identity Center service instance is to be enabled

```
POST https://{hostname}/v1/regions/register

{
  "region_id" : "cn-north-4"
}
```

Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.
409	Conflict.

Error Codes

For details, see **Error Codes**.

4.1.5 Querying Service Instance Status

Function

This API is used to query the status of an IAM Identity Center service instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-center-service/status

Request Parameters

Table 4-26 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-27 Parameters in the response body

Parameter	Type	Description
serviceStatus	String	IAM Identity Center service instance status.
serviceStatusReasons	Array of strings	Reason why the IAM Identity Center service instance is in a state.

Status code: 400

Table 4-28 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-29 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-30 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Querying service instance status

```
GET https://{hostname}/v1/identity-center-service/status
```

Example Response

Status code: 200

Successful

```
{
  "serviceStatus" : "enable",
  "serviceStatusReasons" : "success"
}
```

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.1.6 Enabling an IAM Identity Center Instance

Function

This API is used to enable an IAM Identity Center service instance. It can be called only from the organization's management account.

URI

POST /v1/service/start

Request Parameters

Table 4-31 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-32 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-33 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 409

Table 4-34 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Enabling an IAM Identity Center service instance

```
POST https://{hostname}/v1/service/start
```

Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.
409	Conflict.

Error Codes

For details, see **Error Codes**.

4.1.7 Deleting a Service Instance

Function

This API is used to delete an IAM Identity Center service instance. It can be called only from the organization's management account.

URI

POST /v1/service/delete

Request Parameters

Table 4-35 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-36 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-37 Parameters in the response body

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

Parameter	Type	Description
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-38 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Deleting an IAM Identity Center service instance

```
POST https://{hostname}/v1/service/delete
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.1.8 Setting a Custom Portal URL

Function

This API is used to set a custom portal URL. The default URL format is idcenter.huaweicloud.com/d-*xxxxxxxxxx*/portal. You can change it to idcenter.huaweicloud.com/*your_subdomain*/portal. Setting a custom portal URL is a one-time operation and cannot be undone. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/alias

Table 4-39 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-40 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-41 Parameters in the request body

Parameter	Mandatory	Type	Description
alias	Yes	String	Alias of the user-defined identity source ID.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-42 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-43 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 409

Table 4-44 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Setting a custom portal URL. The default URL format is idcenter.huaweicloud.com/d-*xxxxxxxxxx*/portal. You can change it to idcenter.huaweicloud.com/*your_subdomain*/portal. Setting a custom portal URL is a one-time operation and cannot be undone.

```
POST https://{hostname}/v1/instances/{instance_id}/alias

{
  "alias" : "mycimpany"
}
```


Example Response

None

Status Codes

Status Code	Description
200	Successful
400	Bad request.
403	Forbidden.
409	Conflict.

Error Codes

For details, see **Error Codes**.

4.1.9 Updating HA Function Configurations

Function

This API is used to enable or disable high availability (HA) function configurations. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/instances/{instance_id}/disaster-recovery-configuration

Table 4-45 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-46 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-47 Parameters in the request body

Parameter	Mandatory	Type	Description
disaster_recovery_choice	Yes	String	Whether to enable the HA function.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-48 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-49 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted error message.

Example Request

Enabling or disabling the HA function configurations

```
PUT https://{hostname}/v1/instances/{instance_id}/disaster-recovery-configuration

{
  "disaster_recovery_choice" : "ACCEPT"
}
```

Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.1.10 Querying HA Configurations

Function

This API is used to query configurations of the HA function. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/disaster-recovery-configuration

Table 4-50 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-51 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-52 Parameters in the response body

Parameter	Type	Description
disaster_recovery_choice	String	Whether to enable the HA function.

Status code: 400

Table 4-53 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-54 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying configurations of the HA function

```
GET https://{hostname}/v1/instances/{instance_id}/disaster-recovery-configuration
```

Example Response

Status code: 200

Successful

```
{
  "disaster_recovery_choice" : "REJECT"
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.2 Access Control Attribute Management

4.2.1 Enabling Access Control Attributes for a Specified Instance

Function

This API is used to enable access control attributes for a specified instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/access-control-attribute-configuration

Table 4-55 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-56 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-57 Parameters in the request body

Parameter	Mandatory	Type	Description
instance_access_control_attribute_configuration	Yes	Object	Identity source's attribute to be added to the ABAC configuration in IAM Identity Center.

Table 4-58 instance_access_control_attribute_configuration

Parameter	Mandatory	Type	Description
access_control_attributes	Yes	Array of objects	Attributes configured for ABAC in the IAM Identity Center instance. Array length: **0 - 20**

Table 4-59 access_control_attributes

Parameter	Mandatory	Type	Description
key	Yes	String	Name of the attribute associated with the identity in the identity source. Minimum length: **1** Maximum length: **128**
value	Yes	Object	Mapping the specified attribute to the identity source.

Table 4-60 value

Parameter	Mandatory	Type	Description
source	Yes	Array of strings	Mapping the specified attribute to the identity source. Minimum length: **0** Maximum length: **255** Array length: **1-1**

Response Parameters

Status code: 400

Table 4-61 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-62 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Enabling access control attributes for a specified instance

```
POST https://{hostname}/v1/instances/{instance_id}/access-control-attribute-configuration

{
  "instance_access_control_attribute_configuration" : {
    "access_control_attributes" : [ {
      "key" : "email",
      "value" : {
        "source" : [ "${path:emails[primary eq true].value}" ]
      }
    }, {
      "key" : "displayName",
      "value" : {
        "source" : [ "${path:displayName}" ]
      }
    } ]
  }
}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.2.2 Obtaining Access Control Attributes for a Specified Instance

Function

This API is used to return a list of IAM Identity Center identity source attributes that have been configured to be used with attribute-based access control (ABAC) of a specified IAM Identity Center instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/access-control-attribute-configuration

Table 4-63 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-64 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-65 Parameters in the response body

Parameter	Type	Description
instance_access_control_attribute_configuration	Object	List of IAM Identity Center identity source attributes that have been added to the ABAC configuration.

Parameter	Type	Description
status	String	ABAC attribute configuration status. Enumerated value: • **ENABLED** • **CREATION_IN_PROGRESS** • **CREATION_FAILED**
status_reason	String	Details about the state of the specified attribute.

Table 4-66 instance_access_control_attribute_configuration

Parameter	Type	Description
access_control_attributes	Array of objects	Attributes configured for ABAC in the IAM Identity Center instance. Array length: **0 - 20**

Table 4-67 access_control_attributes

Parameter	Type	Description
key	String	Name of the attribute associated with the identity in the identity source. Minimum length: **1** Maximum length: **128**
value	Object	Mapping the specified attribute to the identity source.

Table 4-68 value

Parameter	Type	Description
source	Array of strings	Mapping the specified attribute to the identity source. Minimum length: **0** Maximum length: **255** Array length: **1-1**

Status code: 400

Table 4-69 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-70 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Obtaining access control attributes for a specified instance

```
GET https://{hostname}/v1/instances/{instance_id}/access-control-attribute-configuration
```

Example Response

Status code: 200

Successful

```
{
  "instance_access_control_attribute_configuration" : {
    "access_control_attributes" : [ {
      "key" : "email",
      "value" : {
        "source" : [ "${path:emails[primary eq true].value}" ]
      }
    }, {
      "key" : "displayName",
      "value" : {
        "source" : [ "${path:displayName}" ]
      }
    } ]
  },
  "status" : "ENABLED",
```



```
  "status_reason" : null
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.2.3 Updating Access Control Attributes for a Specified Instance

Function

This API is used to update IAM Identity Center identity source attributes that can be used with the IAM Identity Center instance for ABAC. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/instances/{instance_id}/access-control-attribute-configuration

Table 4-71 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-72 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-73 Parameters in the request body

Parameter	Mandatory	Type	Description
instance_access_control_attribute_configuration	Yes	Object	Update of ABAC configuration attributes.

Table 4-74 instance_access_control_attribute_configuration

Parameter	Mandatory	Type	Description
access_control_attributes	Yes	Array of objects	Attributes configured for ABAC in the IAM Identity Center instance. Array length: **0 - 20**

Table 4-75 access_control_attributes

Parameter	Mandatory	Type	Description
key	Yes	String	Name of the attribute associated with the identity in the identity source. Minimum length: **1** Maximum length: **128**
value	Yes	Object	Mapping the specified attribute to the identity source.

Table 4-76 value

Parameter	Mandatory	Type	Description
source	Yes	Array of strings	Mapping the specified attribute to the identity source. Minimum length: **0** Maximum length: **255** Array length: **1-1**

Response Parameters

Status code: 400

Table 4-77 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-78 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Updating access control attributes for a specified instance

```
PUT https://{hostname}/v1/instances/{instance_id}/access-control-attribute-configuration

{
  "instance_access_control_attribute_configuration" : {
    "access_control_attributes" : [ {
      "key" : "email",
      "value" : {
        "source" : [ "${path:emails[primary eq true].value}" ]
      }
    }, {
      "key" : "nickName",
      "value" : {
        "source" : [ "${path:nickName}" ]
      }
    } ]
  }
}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.2.4 Disabling Access Control Attributes for a Specified Instance

Function

This API is used to disable ABAC for a specified IAM Identity Center instance and delete all configured attribute mappings. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/instances/{instance_id}/access-control-attribute-configuration

Table 4-79 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-80 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 400

Table 4-81 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-82 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Disabling access control attributes for a specified instance

```
DELETE https://{hostname}/v1/instances/{instance_id}/access-control-attribute-configuration
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3 Permission Set Management

4.3.1 Adding a System-defined Identity Policy

Function

This API is used to add a system-defined identity policy to a specified permission set. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/attach-managed-policy

Table 4-83 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Request Parameters

Table 4-84 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-85 Parameters in the request body

Parameter	Mandatory	Type	Description
managed_policy_id	Yes	String	Unique ID of the IAM system-defined identity policy.
managed_policy_name	No	String	Name of the IAM system-defined identity policy. Minimum length: **1** Maximum length: **128**

Response Parameters

Status code: 400

Table 4-86 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-87 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 409

Table 4-88 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Adding a system-defined identity policy to a specified permission set

```
POST https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}/attach-managed-policy

{
  "managed_policy_id" : "848805579**********03de60620a5",
  "managed_policy_name" : "sys_example_456"
}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.2 Deleting a Permission Set

Function

This API is used to delete a specified permission set according to the permission set ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/instances/{instance_id}/permission-sets/{permission_set_id}

Table 4-89 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Request Parameters

Table 4-90 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 400

Table 4-91 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-92 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-93 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Deleting a specified permission set according to the permission set ID

```
DELETE https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.3 Querying Permission Set Details

Function

This API is used to query details about a specified permission set according to the permission set ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}

Table 4-94 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Request Parameters

Table 4-95 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-96 Parameters in the response body

Parameter	Type	Description
permission_set	Object	Permission set details.

Table 4-97 permission_set

Parameter	Type	Description
created_date	Long	Time when a permission set is created.
description	String	Description of a permission set. Minimum length: **1** Maximum length: **700**
name	String	Name of a permission set. Minimum length: **1** Maximum length: **32**
permission_set_id	String	Unique ID of a permission set.
relay_state	String	Redirection of users within an application during the federated authentication. Minimum length: **1** Maximum length: **240**

Parameter	Type	Description
session_duration	String	Length of time that the application user sessions are valid for in the ISO 8601 standard. Minimum length: **1** Maximum length: **100**
permission_urn	String	URN of a permission set.

Status code: 400

Table 4-98 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-99 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-100 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying details about a specified permission set according to the permission set ID

```
GET https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}
```

Example Response

Status code: 200

Successful

```
{
  "permission_set" : {
    "created_date" : 1684794344964,
    "description" : "Example permission set",
    "name" : "example_0615",
    "permission_set_id" : "ps-8603aaaaaaaa14bd",
    "relay_state" : "",
    "session_duration" : "PT4H",
    "permission_urn" : "IdentityCenter::system:permissionSet:ps-8603aaaaaaaa14bd"
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.4 Updating a Permission Set

Function

This API is used to update the attributes of a specified permission set according to the permission set ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/instances/{instance_id}/permission-sets/{permission_set_id}

Table 4-101 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Request Parameters

Table 4-102 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-103 Parameters in the request body

Parameter	Mandatory	Type	Description
description	No	String	Description of a permission set. Minimum length: **0** Maximum length: **1024**
relay_state	No	String	Redirection of users within an application during the federated authentication. Minimum length: **0** Maximum length: **240**
session_duration	No	String	Length of time that the application user sessions are valid for in the ISO 8601 standard. Minimum length: **1** Maximum length: **100**

Response Parameters

Status code: 400

Table 4-104 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-105 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-106 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Updating the attributes of a specified permission set according to the permission set ID

```
PUT https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}

{
  "description" : "Update an example permission set",
  "relay_state" : "",
  "session_duration" : "PT8H"
}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.5 Deleting a System-defined Identity Policy

Function

This API is used to delete a system-defined identity policy from a specified permission set. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/detach-managed-policy

Table 4-107 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Request Parameters

Table 4-108 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-109 Parameters in the request body

Parameter	Mandatory	Type	Description
managed_policy_id	Yes	String	Unique ID of the IAM system-defined identity policy.

Response Parameters

Status code: 400

Table 4-110 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-111 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-112 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Deleting a system-defined identity policy from a specified permission set

```
POST https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}/detach-managed-policy

{
  "managed_policy_id" : "ps-8603aaaaaaaa14bd"
}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.6 Querying Details About a Custom Identity Policy

Function

This API is used to query details about a custom identity policy in a specified permission set. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}/custom-policy

Table 4-113 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Request Parameters

Table 4-114 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-115 Parameters in the response body

Parameter	Type	Description
custom_policy	String	Custom identity policy added to the permission set. Minimum length: 1 Maximum length: 131,072

Status code: 400

Table 4-116 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-117 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying details about a custom identity policy in a specified permission set

```
GET https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}/custom-policy
```

Example Response

Status code: 200

```
{
  "custom_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Deny\",\"Action\":
[\"organizations:ous:delete\"],\"Condition\":{\"StringEquals\":{\"g:ResourceAccount\":
[\"0a6d25d23900d45c0faac010e0fb4de0\"]}}}]}"
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.7 Adding a Custom Identity Policy

Function

This API is used to add a custom identity policy to a specified permission set. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/instances/{instance_id}/permission-sets/{permission_set_id}/custom-policy

Table 4-118 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Request Parameters

Table 4-119 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-120 Parameters in the request body

Parameter	Mandatory	Type	Description
custom_policy	Yes	String	Custom identity policy added to the permission set. Minimum length: 1 Maximum length: 131,072

Response Parameters

Status code: 400

Table 4-121 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-122 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 409

Table 4-123 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Adding a custom identity policy to a specified permission set

```
PUT https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}/custom-policy
```



```
{
  "custom_policy" : "{\"Version\":\"5.0\",\"Statement\":[{\"Effect\":\"Deny\",\"Action\":
[\"organizations:ous:delete\"],\"Condition\":{\"StringEquals\":{\"g:ResourceAccount\":
[\"0a6d25d23900d45c0faac010e0fb4de0\"]}}}]}"
}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.8 Deleting a Custom Identity Policy

Function

This API is used to delete a custom identity policy from a specified permission set. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/instances/{instance_id}/permission-sets/{permission_set_id}/custom-policy

Table 4-124 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Request Parameters

Table 4-125 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 400

Table 4-126 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-127 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Deleting a custom identity policy from a specified permission set


```
DELETE https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}/custom-policy
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.9 Listing Accounts Associated with a Permission Set

Function

This API is used to list the accounts associated with a specified permission set. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}/accounts

Table 4-128 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Table 4-129 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**

Parameter	Mandatory	Type	Description
provisioning_status	No	String	Provisioning status of a permission set. Enumerated value: • **LATEST_PERMISSION_SET_PROVISIONED** • **LATEST_PERMISSION_SET_NOT_PROVISIONED**

Request Parameters

Table 4-130 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-131 Parameters in the response body

Parameter	Type	Description
account_ids	Array of strings	Account ID list.
page_info	Object	Pagination information.

Table 4-132 page_info

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**.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-133 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-134 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing the accounts associated with a specified permission set

```
GET https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}/accounts
```


Example Response

Status code: 200

Successful

```
{
  "account_ids" : [ "9ced4bf2b81c086cf24fd70c3932f84f" ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.10 Listing System-defined Identity Policies

Function

This API is used to list the system-defined identity policies that are attached to a specified permission set. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}/managed-policies

Table 4-135 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Table 4-136 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**

Request Parameters

Table 4-137 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-138 Parameters in the response body

Parameter	Type	Description
attached_managed_policies	Array of objects	List of IAM system-defined identity policies.
page_info	Object	Pagination information.

Table 4-139 attached_managed_policies

Parameter	Type	Description
policy_id	String	Unique ID of the IAM system-defined identity policy. Minimum length: **20** Maximum length: **2048**
policy_name	String	Name of the IAM system-defined identity policy. Minimum length: **1** Maximum length: **100**

Table 4-140 page_info

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**.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-141 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-142 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing the system-defined identity policies that are attached to a specified permission set

```
GET https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}/managed-policies
```

Example Response

Status code: 200

Successful

```
{
  "attached_managed_policies" : [ {
    "policy_id" : "848805579**********03de60620a5",
    "policy_name" : "sys_example_456"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.11 Listing Pre-provisioning Statuses of Permission Sets

Function

This API is used to list the pre-provisioning statuses of permission sets for a specified instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/permission-sets/provisioning-statuses

Table 4-143 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Table 4-144 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**
status	No	String	Status of the permission set provisioning process. Enumerated value: • **IN_PROGRESS** • **SUCCEEDED** • **FAILED**

Request Parameters

Table 4-145 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-146 Parameters in the response body

Parameter	Type	Description
permission_sets_provisioning_status	Array of objects	Authorization status of a permission set.
page_info	Object	Pagination information.

Table 4-147 permission_sets_provisioning_status

Parameter	Type	Description
created_date	Long	Date when a permission set was created.
request_id	String	Unique ID of a request. Minimum length: **36** Maximum length: **36**
status	String	Authorization status of a permission set. Enumerated value: • **IN_PROGRESS** • **FAILED** • **SUCCEEDED**

Table 4-148 page_info

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**.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-149 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-150 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing the pre-provisioning statuses of permission sets

```
GET https://{hostname}/v1/instances/{instance_id}/permission-sets/provisioning-statuses
```

Example Response

Status code: 200

Successful

```
{
  "permission_sets_provisioning_status" : [ {
    "created_date" : 1677175760379,
    "request_id" : "1c8c7c49238e605a11775963d34cad92",
    "status" : "IN_PROGRESS"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```


Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.12 Listing Permission Sets

Function

This API is used to list the permission sets of a specified instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/permission-sets

Table 4-151 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Table 4-152 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**
permission_set_id	No	String	Globally unique ID of a permission set.
name	No	String	Name of a permission set.

Request Parameters

Table 4-153 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-154 Parameters in the response body

Parameter	Type	Description
permission_sets	Array of objects	Permission set list.
page_info	Object	Pagination information.

Table 4-155 permission_sets

Parameter	Type	Description
created_date	Long	Time when a permission set is created.
description	String	Description of a permission set. Minimum length: **1** Maximum length: **700**
name	String	Name of a permission set. Minimum length: **1** Maximum length: **32**
permission_set_id	String	Unique ID of a permission set.
relay_state	String	Redirection of users within an application during the federated authentication. Minimum length: **1** Maximum length: **240**

Parameter	Type	Description
session_duration	String	Length of time that the application user sessions are valid for in the ISO 8601 standard. Minimum length: **1** Maximum length: **100**
permission_urn	String	URN of a permission set.

Table 4-156 page_info

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**.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-157 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-158 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing the permission sets of a specified instance

```
GET https://{hostname}/v1/instances/{instance_id}/permission-sets
```

Example Response

Status code: 200

Successful

```
{
  "permission_sets" : [ {
    "created_date" : 1677175760379,
"description": " Example permission set 1",
    "name" : "test_ps_1",
    "permission_set_id" : "ps-8603aaaaaaaa14bd",
    "relay_state" : "",
    "session_duration" : "PT4H",
    "permission_urn" : "IdentityCenter::system:permissionSet:ps-8603aaaaaaaa14bd"
  } ],
  "page_info" : {
    "next_marker" : "649040aaaaaaaaaaaa3e3050",
    "current_count" : 1
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.13 Creating a Permission Set

Function

This API is used to create a permission set in a specified IAM Identity Center instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/permission-sets

Table 4-159 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-160 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-161 Parameters in the request body

Parameter	Mandatory	Type	Description
description	No	String	Description of a permission set. Minimum length: **0** Maximum length: **1024**
name	Yes	String	Name of a permission set. Minimum length: **1** Maximum length: **32**
relay_state	No	String	Redirection of users within an application during the federated authentication. Minimum length: **0** Maximum length: **240**
session_duration	No	String	Length of time that the application user sessions are valid for in the ISO 8601 standard. Minimum length: **1** Maximum length: **100**

Parameter	Mandatory	Type	Description
tags	No	Array of objects	Tags to be attached to a permission set. Array length: 0 - 50

Table 4-162 tags

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. Minimum length: **1** Maximum length: **128**
value	Yes	String	Tag value, which can be empty but cannot be **null**. Minimum length: **0** Maximum length: **255**

Response Parameters

Status code: 200

Table 4-163 Parameters in the response body

Parameter	Type	Description
permission_set	Object	Permission set details.

Table 4-164 permission_set

Parameter	Type	Description
created_date	Long	Time when a permission set is created.
description	String	Description of a permission set. Minimum length: **1** Maximum length: **700**
name	String	Name of a permission set. Minimum length: **1** Maximum length: **32**
permission_set_id	String	Unique ID of a permission set.

Parameter	Type	Description
relay_state	String	Redirection of users within an application during the federated authentication. Minimum length: **1** Maximum length: **240**
session_duration	String	Length of time that the application user sessions are valid for in the ISO 8601 standard. Minimum length: **1** Maximum length: **100**
permission_urn	String	URN of a permission set.

Status code: 400

Table 4-165 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-166 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 409

Table 4-167 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Creating a permission set in a specified IAM Identity Center instance

```
POST https://{hostname}/v1/instances/{instance_id}/permission-sets

{
  "description" : "Create an example permission set",
  "name" : "Create a permission set",
  "relay_state" : "",
  "session_duration" : "PT8H",
  "tags" : [ {
    "key" : "tag_k",
    "value" : "tag_v"
  } ]
}
```

Example Response

Status code: 200

Successful

```
{
  "permission_set" : {
    "created_date" : 1677175760379,
    "description" : "Create an example permission set",
    "name" : "Create a permission set",
    "permission_set_id" : "ps-8603aaaaaaaa14bd",
    "relay_state" : "",
    "session_duration" : "PT1H",
    "permission_urn" : "IdentityCenter::system:permissionSet:ps-8603aaaaaaaa14bd"
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.14 Listing Permission Sets Provisioned to an Account

Function

This API is used to list the permission sets provisioned to a specified account. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/permission-sets/provisioned-to-accounts

Table 4-168 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Table 4-169 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**
account_id	Yes	String	Unique ID of a specified account.
provisioning_status	No	String	Authorization status of a permission set. Enumerated value: • **LATEST_PERMISSION_SET_PROVISIONED** • **LATEST_PERMISSION_SET_NOT_PROVISIONED**

Request Parameters

Table 4-170 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-171 Parameters in the response body

Parameter	Type	Description
permission_sets	Array of strings	Permission set ID list that meets the query conditions.
page_info	Object	Pagination information.

Table 4-172 page_info

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**.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-173 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-174 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing the permission sets provisioned to a specified account

```
GET https://{hostname}/v1/instances/{instance_id}/permission-sets/provisioned-to-accounts
```

Example Response

Status code: 200

Successful

```
{
  "permission_sets" : [ "ps-8603aaaaaaaa14bd" ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.15 Pre-provisioning a Permission Set

Function

This API is used to pre-provision a specified permission set to a specified account. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/provision

Table 4-175 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Request Parameters

Table 4-176 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-177 Parameters in the request body

Parameter	Mandatory	Type	Description
target_id	No	String	Account ID.
target_type	Yes	String	Type of the principal to be attached. Enumerated value: • **ACCOUNT** • **ALL_PROVISIONED_ACCOUNTS**

Response Parameters

Status code: 200

Table 4-178 Parameters in the response body

Parameter	Type	Description
permission_set_provisioning_status	Object	Authorization details of a permission set.

Table 4-179 permission_set_provisioning_status

Parameter	Type	Description
account_id	String	Unique ID of a specified account.
created_date	String	Date when a permission set was created.
failure_reason	String	Failure cause.
permission_set_id	String	Unique ID of a permission set.
request_id	String	Unique ID of a request. Minimum length: **36** Maximum length: **36**
status	String	Authorization status of a permission set. Enumerated value: • **IN_PROGRESS** • **FAILED** • **SUCCEEDED**

Status code: 400

Table 4-180 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-181 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-182 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Pre-provisioning a specified permission set to a specified account

```
POST https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}/provision

{
  "target_id" : "5146d03d8aaaaaaaaaaaabbae60620a5",
  "target_type" : "ACCOUNT"
}
```

Example Response

Status code: 200

Successful

```
{
  "permission_set_provisioning_status" : {
    "account_id" : "5146d03d8aaaaaaaaaaaabbae60620a5",
    "created_date" : "1677175760379",
    "failure_reason" : "",
    "permission_set_id" : "ps-8603aaaaaaaa14bd",
    "request_id" : "a1177591c8c7c49238e60563d34cad92",
```



```
    "status" : "SUCCEEDED"
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.16 Querying Pre-attachment Status Details of a Permission Set

Function

This API is used to query the pre-attachment status details of a permission set based on the request ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/permission-sets/provisioning-status/{request_id}

Table 4-183 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
request_id	Yes	String	Unique ID of a request.

Request Parameters

Table 4-184 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-185 Parameters in the response body

Parameter	Type	Description
permission_set_provisioning_status	Object	Authorization details of a permission set.

Table 4-186 permission_set_provisioning_status

Parameter	Type	Description
account_id	String	Unique ID of a specified account.
created_date	String	Date when a permission set was created.
failure_reason	String	Failure cause.
permission_set_id	String	Unique ID of a permission set.
request_id	String	Unique ID of a request. Minimum length: **36** Maximum length: **36**
status	String	Authorization status of a permission set. Enumerated value: • **IN_PROGRESS** • **FAILED** • **SUCCEEDED**

Status code: 400

Table 4-187 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-188 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-189 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying the pre-attachment status details of a permission set based on the request ID

```
GET https://{hostname}/v1/instances/{instance_id}/permission-sets/provisioning-status/{request_id}
```

Example Response

Status code: 200

Successful

```
{
  "permission_set_provisioning_status" : {
    "account_id" : "5146d03d8aaaaaaaaaaabbae60620a5",
    "created_date" : "1677175760379",
    "failure_reason" : "",
    "permission_set_id" : "ps-8603aaaaaaaa14bd",
    "request_id" : "a1177591c8c7c49238e60563d34cad92",
    "status" : "SUCCEEDED"
  }
}
```


Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.17 Adding a System-defined Policy

Function

This API is used to add a system-defined policy to a specified permission set. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/attach-managed-role

Table 4-190 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Request Parameters

Table 4-191 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-192 Parameters in the request body

Parameter	Mandatory	Type	Description
managed_role_id	Yes	String	Unique ID of the IAM system-defined policy.
managed_role_name	No	String	Name of the IAM system-defined policy. Minimum length: **1** Maximum length: **128**

Response Parameters

Status code: 400

Table 4-193 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-194 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 409

Table 4-195 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Adding a system-defined policy to a specified permission set

```
POST https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}/attach-managed-roles

{
  "managed_role_id" : "ba5146848aaaaaaaaaaa03de60620a5",
  "managed_role_name" : "role_example_456"
}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.18 Deleting a System-defined Policy

Function

This API is used to delete a system-defined policy from a specified permission set. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/detach-managed-role

Table 4-196 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Request Parameters

Table 4-197 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-198 Parameters in the request body

Parameter	Mandatory	Type	Description
managed_role_id	Yes	String	Unique ID of the IAM system-defined policy.

Response Parameters

Status code: 400

Table 4-199 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-200 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-201 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Deleting a system-defined policy from a specified permission set

```
POST https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}/detach-managed-roles

{
  "managed_role_id" : "ba5146848aaaaaaaaaaa03de60620a5"
}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.19 Listing System-defined Policies

Function

This API is used to list the system-defined policies that are attached to a specified permission set. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}/managed-roles

Table 4-202 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
permission_set_id	Yes	String	Globally unique ID of a permission set.

Table 4-203 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**

Request Parameters

Table 4-204 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-205 Parameters in the response body

Parameter	Type	Description
attached_managed_roles	Array of objects	List of IAM system-defined policies.
page_info	Object	Pagination information.

Table 4-206 attached_managed_roles

Parameter	Type	Description
role_id	String	Unique ID of the IAM system-defined policy. Minimum length: **20** Maximum length: **2048**
role_name	String	Name of the IAM system-defined policy. Minimum length: **1** Maximum length: **100**

Table 4-207 page_info

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**.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-208 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-209 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing the system-defined policies that are attached to a specified permission set

```
GET https://{hostname}/v1/instances/{instance_id}/permission-sets/{permission_set_id}/managed-roles
```


Example Response

Status code: 200

Successful

```
{
  "attached_managed_roles" : [ {
    "role_id" : "ba5146848aaaaaaaaaaa03de60620a5",
    "role_name" : "role_example_456"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.3.20 Querying Permission Set Quotas

Function

This API is used to query permission set quotas. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/permission-set-summary

Table 4-210 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-211 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-212 Parameters in the response body

Parameter	Type	Description
permission_sets	Long	Number of created permission sets.
permission_sets_quota	Long	Quota of permission sets.
permission_policy_count_quota	Long	Quota of policies that can be bound to a permission set.
permission_policy_quota	Long	Quota of identity policies that can be bound to a permission set.

Status code: 400

Table 4-213 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-214 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying permission set quotas

```
GET https://{hostname}/v1/instances/{instance_id}/permission-set-summary
```

Example Response

Status code: 200

Successful

```
{
  "permission_sets" : 50,
  "permission_sets_quota" : 20,
  "permission_policy_count_quota" : 20,
  "permission_policy_quota" : 10
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.4 Account Assignment Management

4.4.1 Removing Account Assignments

Function

This API is used to remove a principal's access from a specified account using a specified permission set. The principal can be either a user or a group in IAM Identity Center. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/account-assignments/delete

Table 4-215 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-216 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-217 Parameters in the request body

Parameter	Mandatory	Type	Description
permission_set_id	Yes	String	Unique ID of a permission set.
principal_id	Yes	String	Unique ID of a principal (for example, a user or group) in IAM Identity Center.
principal_type	Yes	String	Principal type. Enumerated value: • **USER** • **GROUP**

Parameter	Mandatory	Type	Description
target_id	Yes	String	ID of the target account.
target_type	Yes	String	Target type. Enumerated value: • **ACCOUNT**

Response Parameters

Status code: 200

Table 4-218 Parameters in the response body

Parameter	Type	Description
account_assignment_deletion_status	Object	Status object for the account assignment deletion operation.

Table 4-219 account_assignment_deletion_status

Parameter	Type	Description
created_date	Long	Creation date.
failure_reason	String	Failure cause.
permission_set_id	String	Unique ID of a permission set.
principal_id	String	Unique ID of a principal (for example, a user or group) in IAM Identity Center.
principal_type	String	Principal type of an operation. Enumerated value: • **USER** • **GROUP**
request_id	String	Unique ID of a request.
status	String	Authorization status of a permission set. Enumerated value: • **IN_PROGRESS** • **FAILED** • **SUCCEEDED**
target_id	String	Unique ID of a target principal.

Parameter	Type	Description
target_type	String	Principal type. Enumerated value: • **ACCOUNT**

Status code: 400

Table 4-220 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-221 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-222 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted error message.

Status code: 409

Table 4-223 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Removing an IAM Identity Center user access from a specified account using a specified permission set

```
POST https://{hostname}/v1/instances/{instance_id}/account-assignments/delete

{
  "permission_set_id" : "848805579**********03de60620a5",
  "principal_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
  "principal_type" : "USER",
  "target_id" : "5146d03d8aaaaaaaaaaaabbae60620a5",
  "target_type" : "ACCOUNT"
}
```

Example Response

Status code: 200

Successful

```
{
  "account_assignment_deletion_status" : {
    "created_date" : 0,
    "failure_reason" : "string",
    "permission_set_id" : "string",
    "principal_id" : "string",
    "principal_type" : "USER",
    "request_id" : "string",
    "status" : "IN_PROGRESS",
    "target_id" : "string",
    "target_type" : "ACCOUNT"
  }
}
```


Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.4.2 Querying Details about the Account Assignment Creation Status

Function

This API is used to query details about the account assignment creation status of a specified IAM Identity Center instance based on the request ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/account-assignments/creation-status/{request_id}

Table 4-224 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
request_id	Yes	String	Unique ID of a request.

Request Parameters

Table 4-225 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-226 Parameters in the response body

Parameter	Type	Description
account_assignment_creation_status	Object	Status object for the account assignment creation operation.

Table 4-227 account_assignment_creation_status

Parameter	Type	Description
created_date	Long	Creation date.
failure_reason	String	Failure cause.
permission_set_id	String	Unique ID of a permission set.
principal_id	String	Unique ID of a principal (for example, a user or group) in IAM Identity Center.
principal_type	String	Principal type of an operation. Enumerated value: • **USER** • **GROUP**
request_id	String	Unique ID of a request.
status	String	Authorization status of a permission set. Enumerated value: • **IN_PROGRESS** • **FAILED** • **SUCCEEDED**
target_id	String	Unique ID of a target principal.
target_type	String	Principal type. Enumerated value: • **ACCOUNT**

Status code: 400

Table 4-228 Parameters in the response body

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

Parameter	Type	Description
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-229 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-230 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying details about the account assignment creation status of a specified IAM Identity Center instance based on the request ID

```
GET https://{hostname}/v1/instances/{instance_id}/account-assignments/creation-status/{request_id}
```

Example Response

Status code: 200

Successful

```
{
  "account_assignment_creation_status" : {
    "created_date" : 1677175760379,
    "failure_reason" : "",
    "permission_set_id" : "ps-8603aaaaaaaa14bd",
    "principal_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
    "principal_type" : "USER",
    "request_id" : "9238e6aaaaaaaaaaaaaaaaaaaa4cad92",
    "status" : "IN_PROGRESS",
    "target_id" : "5146d03d8aaaaaaaaaaaabbae60620a5",
    "target_type" : "ACCOUNT"
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.4.3 Listing Account Assignment Creation Statuses

Function

This API is used to list the account assignment creation statuses of a specified IAM Identity Center instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/account-assignments/creation-statuses

Table 4-231 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Table 4-232 Query parameters

Parameter	Mandatory	Type	Description
status	No	String	Status of the listing account assignment creation process. Enumerated value: • **IN_PROGRESS** • **SUCCEEDED** • **FAILED**
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**

Request Parameters

Table 4-233 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-234 Parameters in the response body

Parameter	Type	Description
account_assignments_creation_status	Array of objects	Operation status list.
page_info	Object	Pagination information.

Table 4-235 account_assignments_creation_status

Parameter	Type	Description
created_date	Long	Creation date.
request_id	String	Unique ID of a request.
status	String	Authorization status of a permission set. Enumerated value: • **IN_PROGRESS** • **FAILED** • **SUCCEEDED**

Table 4-236 page_info

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**.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-237 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-238 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing the account assignment creation statuses of a specified IAM Identity Center instance

```
GET https://{hostname}/v1/instances/{instance_id}/account-assignments/creation-statuses
```

Example Response

Status code: 200

Successful

```
{
  "account_assignments_creation_status" : [ {
    "created_date" : 1677175760379,
    "request_id" : "9238e6aaaaaaaaaaaaaaaaaaaa4cad92",
    "status" : "IN_PROGRESS"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.4.4 Listing Account Assignment Deletion Statuses

Function

This API is used to list the account assignment deletion statuses of a specified IAM Identity Center instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/account-assignments/deletion-statuses

Table 4-239 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Table 4-240 Query parameters

Parameter	Mandatory	Type	Description
status	No	String	Status of the listing account assignment deletion process. Enumerated value: • **IN_PROGRESS** • **SUCCEEDED** • **FAILED**
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**

Request Parameters

Table 4-241 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-242 Parameters in the response body

Parameter	Type	Description
account_assignments_deletion_status	Array of objects	Operation status list.
page_info	Object	Pagination information.

Table 4-243 account_assignments_deletion_status

Parameter	Type	Description
created_date	Long	Creation date.
request_id	String	Unique ID of a request.
status	String	Authorization status of a permission set. Enumerated value: • **IN_PROGRESS** • **FAILED** • **SUCCEEDED**

Table 4-244 page_info

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**.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-245 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-246 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing the account assignment deletion statuses of a specified IAM Identity Center instance

```
GET https://{hostname}/v1/instances/{instance_id}/account-assignments/deletion-statuses
```

Example Response

Status code: 200

Successful

```
{
  "account_assignments_deletion_status" : [ {
    "created_date" : 1677175760379,
    "request_id" : "9238e6aaaaaaaaaaaaaaaaaaa4cad92",
    "status" : "IN_PROGRESS"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```


Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.4.5 Listing Users or Groups Associated with an Account and a Permission Set

Function

This API is used to list the users or groups associated with a specified account and a specified permission set. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/account-assignments

Table 4-247 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Table 4-248 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**
account_id	Yes	String	Unique ID of a specified account.
permission_set_id	No	String	Unique ID of a specified permission set.

Request Parameters

Table 4-249 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-250 Parameters in the response body

Parameter	Type	Description
account_assignments	Array of objects	Listed account assignments.
page_info	Object	Pagination information.

Table 4-251 account_assignments

Parameter	Type	Description
account_id	String	Unique ID of an account.
permission_set_id	String	Unique ID of a permission set.
principal_id	String	Unique ID of a principal (for example, a user or group) in IAM Identity Center.
principal_type	String	Associated principal type. Enumerated value: • **USER** • **GROUP**

Table 4-252 page_info

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**.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-253 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-254 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing the users or groups associated with a specified account and a specified permission set


```
GET https://{hostname}/v1/instances/{instance_id}/account-assignments
```

Example Response

Status code: 200

Successful

```
{
  "account_assignments" : [ {
    "account_id" : "5146d03d8aaaaaaaaaaaabbae60620a5",
    "permission_set_id" : "ps-8603aaaaaaaa14bd",
    "principal_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
    "principal_type" : "USER"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.4.6 Creating Account Assignments

Function

This API is used to assign access permissions to a principal for a specified account using a specified permission set. The principal can be either a user or a group in IAM Identity Center. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/account-assignments/create

Table 4-255 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-256 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-257 Parameters in the request body

Parameter	Mandatory	Type	Description
permission_set_id	Yes	String	Unique ID of a permission set.
principal_id	Yes	String	Unique ID of a principal (for example, a user or group) in IAM Identity Center.
principal_type	Yes	String	Principal type for which the assignment will be created. Enumerated value: • **USER** • **GROUP**
target_id	Yes	String	ID of the target principal.
target_type	Yes	String	Principal type for which the assignment will be created. Enumerated value: • **ACCOUNT**

Response Parameters

Status code: 200

Table 4-258 Parameters in the response body

Parameter	Type	Description
account_assignment_creation_status	Object	Status object for the account assignment creation operation.

Table 4-259 account_assignment_creation_status

Parameter	Type	Description
created_date	Long	Creation date.
failure_reason	String	Failure cause.
permission_set_id	String	Unique ID of a permission set.
principal_id	String	Unique ID of a principal (for example, a user or group) in IAM Identity Center.
principal_type	String	Principal type of an operation. Enumerated value: • **USER** • **GROUP**
request_id	String	Unique ID of a request.
status	String	Authorization status of a permission set. Enumerated value: • **IN_PROGRESS** • **FAILED** • **SUCCEEDED**
target_id	String	Unique ID of a target principal.
target_type	String	Principal type. Enumerated value: • **ACCOUNT**

Status code: 400

Table 4-260 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-261 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-262 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Assigning access permissions to an IAM Identity Center user for a specified account using a specified permission set

```
POST https://{hostname}/v1/instances/{instance_id}/account-assignments/create

{
  "permission_set_id" : "848805579**********03de60620a5",
  "principal_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
  "principal_type" : "USER",
  "target_id" : "5146d03d8aaaaaaaaaaaabbae60620a5",
  "target_type" : "ACCOUNT"
}
```

Example Response

Status code: 200

Successful

```
{
  "account_assignment_creation_status" : {
    "created_date" : 0,
    "failure_reason" : "string",
    "permission_set_id" : "string",
```



```
    "principal_id" : "string",
    "principal_type" : "USER",
    "request_id" : "string",
    "status" : "IN_PROGRESS",
    "target_id" : "string",
    "target_type" : "ACCOUNT"
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.4.7 Querying Details about the Account Assignment Deletion Status

Function

This API is used to query details about the account assignment deletion status of a specified IAM Identity Center instance based on the request ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/account-assignments/deletion-status/{request_id}

Table 4-263 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
request_id	Yes	String	Unique ID of a request.

Request Parameters

Table 4-264 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-265 Parameters in the response body

Parameter	Type	Description
account_assignment_deletion_status	Object	Status object for the account assignment deletion operation.

Table 4-266 account_assignment_deletion_status

Parameter	Type	Description
created_date	Long	Creation date.
failure_reason	String	Failure cause.
permission_set_id	String	Unique ID of a permission set.
principal_id	String	Unique ID of a principal (for example, a user or group) in IAM Identity Center.
principal_type	String	Principal type of an operation. Enumerated value: • **USER** • **GROUP**
request_id	String	Unique ID of a request.
status	String	Authorization status of a permission set. Enumerated value: • **IN_PROGRESS** • **FAILED** • **SUCCEEDED**
target_id	String	Unique ID of a target principal.
target_type	String	Principal type. Enumerated value: • **ACCOUNT**

Status code: 400

Table 4-267 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 403

Table 4-268 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-269 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying details about the account assignment deletion status of a specified IAM Identity Center instance based on the request ID

```
GET https://{hostname}/v1/instances/{instance_id}/account-assignments/deletion-status/{request_id}
```


Example Response

Status code: 200

Successful

```
{
  "account_assignment_deletion_status" : {
    "created_date" : 1677175760379,
    "failure_reason" : "",
    "permission_set_id" : "ps-8603aaaaaaaa14bd",
    "principal_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
    "principal_type" : "USER",
    "request_id" : "9238e6aaaaaaaaaaaaaaaaaaaa4cad92",
    "status" : "IN_PROGRESS",
    "target_id" : "5146d03d8aaaaaaaaaaaabbae60620a5",
    "target_type" : "ACCOUNT"
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.4.8 Listing Accounts Associated with a User or User Group

Function

This API is used to list accounts associated with a user or user group. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/account-assignments-for-principals

Table 4-270 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Table 4-271 Query parameters

Parameter	Mandatory	Type	Description
principal_id	Yes	String	Globally unique ID of an IAM Identity Center principal.

Parameter	Mandatory	Type	Description
principal_type	Yes	String	IAM Identity Center principal type.
limit	No	Integer	Maximum number of results returned for each request.
marker	No	String	Pagination marker.
account_id	No	String	Unique ID of a specified account.

Request Parameters

Table 4-272 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-273 Parameters in the response body

Parameter	Type	Description
account_assignments	Array of **AccountAssignmentDto** objects	List of account assignments that meet the search criteria.
page_info	**PageInfoDto** object	Pagination information.

Table 4-274 AccountAssignmentDto

Parameter	Type	Description
account_id	String	Unique ID of an account.
permission_set_id	String	Unique ID of a permission set.

Parameter	Type	Description
principal_id	String	Unique ID of a principal (for example, a user or group) in IAM Identity Center.
principal_type	String	Associated principal type.

Table 4-275 PageInfoDto

Parameter	Type	Description
next_marker	String	If present, more output is available than that included in the current response. To get the next part of the output, use this value in the request parameter in a subsequent call to the same API. You should repeat calling until the **next_marker** parameter is null in a response.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-276 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-277 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing accounts associated with a user or user group

```
GET https://{hostname}/v1/instances/{instance_id}/account-assignments-for-principals
```

Example Response

Status code: 200

Successful

```
{
  "account_assignments" : [ {
    "account_id" : "8c1eef3a241945f69c3d3a6b0252e783",
    "permission_set_id" : "ps-389b8cf93d6aa3ad",
    "principal_id" : "4b969bc6-e8ed-47ce-b62b-936319e2bcb1",
    "principal_type" : "USER"
  }, {
    "account_id" : "8c1eef3a241945f69c3d3a6b0252e783",
    "permission_set_id" : "ps-e0edd386c8e95a4c",
    "principal_id" : "4b969bc6-e8ed-47ce-b62b-936319e2bcb1",
    "principal_type" : "USER"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 2
  }
}
```

Status Codes

Status Codes	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.4.9 Disassociating All Account Authorizations from a User or Group

Function

This API is used to disassociate all account authorizations from a user or group. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/disassociate-profile

Table 4-278 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-279 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-280 Parameters in the request body

Parameter	Mandatory	Type	Description
id	Yes	String	Unique ID of a user or a group.
accessor_type	Yes	String	Type of the principal (a user or a group) to be disassociated.
identity_store_id	Yes	String	Globally ID of the identity source associated with an IAM Identity Center instance.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-281 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-282 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Disassociating all account authorizations from a user or group

```
POST https://{hostname}/v1/instances/{instance_id}/disassociate-profile

{
  "id" : "9190-9834-xxxx",
  "accessor_type" : "USER",
  "identity_store_id" : "d-xxxxxxx"
}
```

Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.5 Tag Management

4.5.1 Listing Tags for the Specified Resource

Function

This API is used to list the tags that are attached to the specified resource. Currently, tags can only be attached to permission sets. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{resource_type}/{resource_id}/tags

Table 4-283 Path parameters

Parameter	Mandatory	Type	Description
resource_type	Yes	String	Resource type. Enumerated value: • **identitycenter:permissionset** (permission set)
resource_id	Yes	String	Unique ID of a permission set. Maximum length: **130**

Table 4-284 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**

Request Parameters

Table 4-285 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-286 Parameters in the response body

Parameter	Type	Description
tags	Array of objects	List of tags.
page_info	Object	Pagination information.

Table 4-287 tags

Parameter	Type	Description
key	String	Tag key. Minimum length: **1** Maximum length: **128**
value	String	Tag value, which can be empty but cannot be **null**. Minimum length: **0** Maximum length: **255**

Table 4-288 page_info

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 until the **next_marker** response element comes back as **null**.
current_count	Integer	Number of records returned on the current page.

Example Request

Listing the tags that are attached to the specified resource

```
GET https://{hostname}/v1/instances/{resource_type}/{resource_id}/tags
```

Example Response

Status code: 200

Successful.

```
{
  "tags" : [ {
    "key" : "auto09230Uv5key",
    "value" : "auto0923XXFmvalue"
  } ],
  "page_info" : {
    "next_marker" : "5f13d2346712e4890abc5678",
    "current_count" : 10
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.5.2 Adding Tags to the Specified Resource

Function

This API is used to add one or more tags to the specified resource. Currently, tags can only be attached to permission sets. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{resource_type}/{resource_id}/tags/create

Table 4-289 Path parameters

Parameter	Mandatory	Type	Description
resource_type	Yes	String	Resource type. Enumerated value: • **identitycenter:permissionset** (permission set)
resource_id	Yes	String	Unique ID of a permission set. Maximum length: **130**

Request Parameters

Table 4-290 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-291 Parameters in the request body

Parameter	Mandatory	Type	Description
tags	Yes	Array of objects	A key-value pair used to manage resources. Array length: 0 - 50

Table 4-292 tags

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. Minimum length: **1** Maximum length: **128**
value	Yes	String	Tag value, which can be empty but cannot be **null**. Minimum length: **0** Maximum length: **255**

Response Parameters

None.

Example Request

Adding tags to the specified resource

```
POST https://{hostname}/v1/instances/{resource_type}/{resource_id}/tags/create

{
  "tags" : [ {
    "key" : "keystring",
    "value" : "valuestring"
  } ]
}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.5.3 Removing the Specified Tag from the Specified Resource

Function

This API is used to remove the specified tag from the specified resource. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{resource_type}/{resource_id}/tags/delete

Table 4-293 Path parameters

Parameter	Mandatory	Type	Description
resource_type	Yes	String	Resource type. Enumerated value: • **identitycenter:permissionset** (permission set)
resource_id	Yes	String	Unique ID of a permission set. Maximum length: **130**

Request Parameters

Table 4-294 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-295 Parameters in the request body

Parameter	Mandatory	Type	Description
tags	Yes	Array of objects	A key-value pair used to manage resources. Array length: **1-20**

Table 4-296 tags

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. Minimum length: **1** Maximum length: **128**
value	No	String	Tag value, which can be empty but cannot be **null**. Minimum length: **0** Maximum length: **255**

Response Parameters

None.

Example Request

Removing the specified tag from the specified resource

```
POST https://{hostname}/v1/instances/{resource_type}/{resource_id}/tags/delete

{
  "tags" : [ {
    "key" : "keystring",
    "value" : "valuestring"
  } ]
}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.6 Application Management

4.6.1 Creating an Application Instance

Function

This API is used to create an application instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/application-instances

Table 4-297 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-298 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-299 Parameters in the request body

Parameter	Mandatory	Type	Description
name	Yes	String	Application instance UUID.
template_id	Yes	String	Application template ID.

Response Parameters

Status code: 201

Table 4-300 Parameters in the response body

Parameter	Type	Description
application_instance	**ApplicationInstanceDto** object	Application instance.

Table 4-301 ApplicationInstanceDto

Parameter	Type	Description
active_certificate	**CertificateDto** object	Activated certificates.
display	**DisplayDto** object	Display information of an application.
identity_provider_config	**IdentityProvider-ConfigDto** object	Identity provider configuration.
application_instance_id	String	Unique ID of an application instance.
name	String	Application UUID.
visible	Boolean	Whether an application is visible on the user portal.
response_config	**ResponseConfigDto** object	Application attribute configuration.
response_schema_config	**ResponseSchemaConfigDto** object	Configuration for application schema attribute mapping.
security_config	**SecurityConfigDto** object	Certificate configuration.
status	String	Application instance status.
template	**ApplicationTemplateDto** object	Information about the template that an application depends on.
service_provider_config	**ServiceProvider-ConfigDto** object	Service provider configuration.
client_id	String	OIDC client ID.
end_user_visible	Boolean	Visible to users or not.
managed_account	String	Account ID of a group member.

Table 4-302 CertificateDto

Parameter	Type	Description
algorithm	String	Certificate generation algorithm.
certificate	String	Application certificate.
certificate_id	String	Application certificate ID.
expiry_date	Long	Certificate expiration time.
status	String	Certificate status.

Parameter	Type	Description
key_size	String	Key size.
issue_date	Long	Certificate generation time.

Table 4-303 IdentityProviderConfigDto

Parameter	Type	Description
issuer_url	String	Identity provider issuer.
metadata_url	String	Identity provider metadata.
remote_login_url	String	Remote login link of an identity provider.
remote_logout_url	String	Remote logout link of an identity provider.

Table 4-304 ApplicationTemplateDto

Parameter	Type	Description
application	**ApplicationTemplateDisplayDto** object	Display information of an application template.
response_config	**ResponseConfigDto** object	Application attribute configuration.
response_schema_config	**ResponseSchemaConfigDto** object	Mapping configuration of application attributes.
sso_protocol	String	Supported protocols.
security_config	**SecurityConfigDto** object	Certificate configuration.
service_provider_config	**ServiceProviderConfigDto** object	Service provider configuration.
template_id	String	Unique ID of an application template.
template_version	String	Application template version.

Table 4-305 ApplicationTemplateDisplayDto

Parameter	Type	Description
application_id	String	Application ID. Its prefix is **app-**.

Parameter	Type	Description
display	**DisplayDto** object	Display information of an application.
application_type	String	Application type.

Table 4-306 DisplayDto

Parameter	Type	Description
description	String	Application description.
display_name	String	Application display name.
icon	String	Application icon.

Table 4-307 ResponseConfigDto

Parameter	Type	Description
properties	Map<String,**ResponseSourceDetailsDto**>	Additional configuration for attribute mapping.
subject	**ResponseSourceDetailsDto** object	Subject attribute mapping configuration.
relay_state	String	Relay state.
ttl	String	Session expiration time.

Table 4-308 ResponseSourceDetailsDto

Parameter	Type	Description
source	Array of strings	Attribute mapping value.

Table 4-309 ResponseSchemaConfigDto

Parameter	Type	Description
properties	Map<String,**ResponseSchemaPropertiesDetailsDto**>	Additional schema configuration for attribute mapping.
subject	**ResponseSchemaSubjectDetailsDto** object	Schema configuration for subject attribute mapping.

Parameter	Type	Description
supported_name_id_formats	Array of strings	Subject NameID format supported by an application.

Table 4-310 ResponseSchemaPropertiesDetailsDto

Parameter	Type	Description
attr_name_format	String	Additional attribute format.
include	String	Whether additional attributes are included.

Table 4-311 ResponseSchemaSubjectDetailsDto

Parameter	Type	Description
name_id_format	String	NameID format.
include	String	Whether NameID is included.

Table 4-312 SecurityConfigDto

Parameter	Type	Description
ttl	String	Certificate expiration time.

Table 4-313 ServiceProviderConfigDto

Parameter	Type	Description
audience	String	SAML audience.
require_request_signature	Boolean	Whether a signature is required.
consumers	Array of **ConsumersDto** objects	SAML response recipient.
start_url	String	Application startup URL.

Table 4-314 ConsumersDto

Parameter	Type	Description
binding	String	SAML transmission protocol.
default_value	Boolean	Whether it is the default recipient.
location	String	SAML ACS URL.

Status code: 400

Table 4-315 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-316 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 409

Table 4-317 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Creating an application instance

```
POST https://{hostname}/v1/instances/{instance_id}/application-instances

{
  "name" : "a689ebed-1b68-44b0-af97-xxxxx",
  "template_id" : "tpl-88f215b39bfcxxxx"
}
```

Example Response

Status code: 201

Successful

```
{
  "application_instance" : {
    "active_certificate" : {
      "algorithm" : "SHA256withRSA",
      "certificate" : "certificate",
      "certificate_id" : "cer-ea56cf20-4ec3-445a-883f-eb70f35fe7d1",
      "expiry_date" : 1911427200000,
      "status" : "ACTIVE",
      "key_size" : "3072",
      "issue_date" : 1753695145064
    },
    "display" : {
      "description" : "Custom SAML 2.0 application",
      "display_name" : "Custom SAML 2.0 application",
      "icon" : ""
    },
    "identity_provider_config" : {
      "issuer_url" : "https://idcenter.ulanqab.huawei.com/v1/saml/assertion/
OGMxZWVmM2EyNDE5NDVmNjljM2QzYTZiMDI1MmU3ODNfZC05NDE0MDdiNGIzX2FwcC1pbnMtYTAzM2
M5MDcwMTZhNTlhZQ==",
      "metadata_url" : "https://idcenter.ulanqab.huawei.com/v1/saml/metadata/
OGMxZWVmM2EyNDE5NDVmNjljM2QzYTZiMDI1MmU3ODNfZC05NDE0MDdiNGIzX2FwcC1pbnMtYTAzM2
M5MDcwMTZhNTlhZQ==",
      "remote_login_url" : "https://idcenter.ulanqab.huawei.com/v1/saml/assertion/
OGMxZWVmM2EyNDE5NDVmNjljM2QzYTZiMDI1MmU3ODNfZC05NDE0MDdiNGIzX2FwcC1pbnMtYTAzM2
M5MDcwMTZhNTlhZQ==",
      "remote_logout_url" : "https://idcenter.ulanqab.huawei.com/v1/saml/logout/
OGMxZWVmM2EyNDE5NDVmNjljM2QzYTZiMDI1MmU3ODNfZC05NDE0MDdiNGIzX2FwcC1pbnMtYTAzM2
M5MDcwMTZhNTlhZQ=="
    },
    "application_instance_id" : "app-ins-a033c907016a59ae",
    "name" : "a689ebed-1b68-44b0-af97-0be880c30127",
    "visible" : true,
    "response_config" : {
      "properties" : { },
      "subject" : null,
      "relay_state" : null,
      "ttl" : "PT1H"
    },
    "response_schema_config" : {
      "properties" : { },
      "subject" : null,
      "supported_name_id_formats" : null
    },
    "security_config" : {
      "ttl" : "P5Y"
    },
    "status" : "CREATED",
    "template" : {
      "application" : {
        "application_id" : "app-ff1258a63a4axxxx",
```



```
      "display" : {
        "description" : "Custom SAML 2.0 application",
        "display_name" : "Custom SAML 2.0 application",
        "icon" : ""
      },
      "application_type" : ""
    },
    "response_config" : {
      "properties" : { },
      "subject" : null,
      "relay_state" : null,
      "ttl" : "PT1H"
    },
    "response_schema_config" : {
      "properties" : { },
      "subject" : null,
      "supported_name_id_formats" : null
    },
    "sso_protocol" : "SAML",
    "security_config" : {
      "ttl" : null
    },
    "service_provider_config" : {
      "audience" : null,
      "require_request_signature" : false,
      "consumers" : null,
      "start_url" : null
    },
    "template_id" : "tpl-88f215b39bfc7575",
    "template_version" : "1"
  },
  "service_provider_config" : {
    "audience" : null,
    "require_request_signature" : false,
    "consumers" : null,
    "start_url" : null
  },
  "client_id" : null,
  "end_user_visible" : null,
  "managed_account" : "8c1eef3a241945f69c3d3a6b0252e783"
 }
}
```


Status Codes

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

Error Codes

For details, see **Error Codes**.

4.6.2 Listing Application Instances

Function

This API is used to list application instances. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/application-instances

Table 4-318 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Table 4-319 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request.
marker	No	String	Pagination marker.

Request Parameters

Table 4-320 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-321 Parameters in the response body

Parameter	Type	Description
application_instances	Array of **ApplicationInstanceDto** objects	List of application instances.
page_info	**PageInfoDto** object	Pagination information.

Table 4-322 ApplicationInstanceDto

Parameter	Type	Description
active_certificate	**CertificateDto** object	Activated certificates.
display	**DisplayDto** object	Display information of an application.
identity_provider_config	**IdentityProvider-ConfigDto** object	Identity provider configuration.
application_instance_id	String	Unique ID of an application instance.
name	String	Application UUID.
visible	Boolean	Whether an application is visible on the user portal.
response_config	**ResponseConfigDto** object	Application attribute configuration.
response_schema_config	**ResponseSchemaConfigDto** object	Configuration for application schema attribute mapping.
security_config	**SecurityConfigD-to** object	Certificate configuration.
status	String	Application instance status.
template	**ApplicationTemplateDto** object	Information about the template that an application depends on.
service_provider_config	**ServiceProvider-ConfigDto** object	Service provider configuration.
client_id	String	OIDC client ID.
end_user_visible	Boolean	Visible to users or not.
managed_account	String	Account ID of a group member.

Table 4-323 CertificateDto

Parameter	Type	Description
algorithm	String	Certificate generation algorithm.
certificate	String	Application certificate.
certificate_id	String	Application certificate ID.
expiry_date	Long	Certificate expiration time.
status	String	Certificate status.
key_size	String	Key size.
issue_date	Long	Certificate generation time.

Table 4-324 IdentityProviderConfigDto

Parameter	Type	Description
issuer_url	String	Identity provider issuer.
metadata_url	String	Identity provider metadata.
remote_login_url	String	Remote login link of an identity provider.
remote_logout_url	String	Remote logout link of an identity provider.

Table 4-325 ApplicationTemplateDto

Parameter	Type	Description
application	**ApplicationTemplateDisplayDto** object	Display information of an application template.
response_config	**ResponseConfigDto** object	Application attribute configuration.
response_schema_config	**ResponseSchemaConfigDto** object	Mapping configuration of application attributes.
sso_protocol	String	Supported protocols.
security_config	**SecurityConfigDto** object	Certificate configuration.
service_provider_config	**ServiceProviderConfigDto** object	Service provider configuration.

Parameter	Type	Description
template_id	String	Unique ID of an application template.
template_version	String	Application template version.

Table 4-326 ApplicationTemplateDisplayDto

Parameter	Type	Description
application_id	String	Application ID. Its prefix is **app-**.
display	**DisplayDto** object	Display information of an application.
application_type	String	Application type.

Table 4-327 DisplayDto

Parameter	Type	Description
description	String	Application description.
display_name	String	Application display name.
icon	String	Application icon.

Table 4-328 ResponseConfigDto

Parameter	Type	Description
properties	Map<String,**ResponseSourceDetailsDto**>	Additional configuration for attribute mapping.
subject	**ResponseSourceDetailsDto** object	Subject attribute mapping configuration.
relay_state	String	Relay state.
ttl	String	Session expiration time.

Table 4-329 ResponseSourceDetailsDto

Parameter	Type	Description
source	Array of strings	Attribute mapping value.

Table 4-330 ResponseSchemaConfigDto

Parameter	Type	Description
properties	Map<String,**ResponseSchemaPropertiesDetailsDto**>	Additional schema configuration for attribute mapping.
subject	**ResponseSchemaSubjectDetailsDto** object	Schema configuration for subject attribute mapping.
supported_name_id_formats	Array of strings	Subject NameID format supported by an application.

Table 4-331 ResponseSchemaPropertiesDetailsDto

Parameter	Type	Description
attr_name_format	String	Additional attribute format.
include	String	Whether additional attributes are included.

Table 4-332 ResponseSchemaSubjectDetailsDto

Parameter	Type	Description
name_id_format	String	NameID format.
include	String	Whether NameID is included.

Table 4-333 SecurityConfigDto

Parameter	Type	Description
ttl	String	Certificate expiration time.

Table 4-334 ServiceProviderConfigDto

Parameter	Type	Description
audience	String	SAML audience.
require_request_signature	Boolean	Whether a signature is required.

Parameter	Type	Description
consumers	Array of **ConsumersDto** objects	SAML response recipient.
start_url	String	Application startup URL.

Table 4-335 ConsumersDto

Parameter	Type	Description
binding	String	SAML transmission protocol.
default_value	Boolean	Whether it is the default recipient.
location	String	SAML ACS URL.

Table 4-336 PageInfoDto

Parameter	Type	Description
next_marker	String	If present, more output is available than that included in the current response. To get the next part of the output, use this value in the request parameter in a subsequent call to the same API. You should repeat calling until the **next_marker** parameter is null in a response.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-337 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-338 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing application instances

```
GET https://{hostname}/v1/instances/{instance_id}/application-instances
```

Example Response

Status code: 200

Successful

```
{
  "applications" : [ {
    "application_urn" : "IdentityCenter::8c1eef3a241945f69xxxxxxx:application:ins-36xxxxxxx/apl-e7f300xxxxx",
    "application_provider_urn" : "IdentityCenter:::applicationProvider:custom-saml",
    "assignment_config" : {
      "assignment_required" : true
    },
    "created_date" : 1752041671967,
    "description" : "ApplicationStartUrl",
    "instance_urn" : "IdentityCenter::8c1eef3a241xxxxx:instance:ins-36218exxxxxxx",
    "name" : "ApplicationStartUrl",
    "portal_options" : {
      "visible" : true,
      "visibility" : "ENABLED",
      "sign_in_options" : {
        "origin" : "IDENTITY_CENTER",
        "application_url" : ""
      }
    },
    "status" : "ENABLED",
    "application_account" : "8c1eef3a241xxxxxx"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful.

Status Code	Description
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.6.3 Listing Preset Application Templates in the Application Directory

Function

This API is used to list preset application templates in the application directory. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/catalog/applications

Table 4-339 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request.
marker	No	String	Pagination marker.

Request Parameters

Table 4-340 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-341 Parameters in the response body

Parameter	Type	Description
applications	Array of **ApplicationTemplateDisplayDto** objects	Application list in the application directory.
page_info	**PageInfoDto** object	Pagination information.

Table 4-342 ApplicationTemplateDisplayDto

Parameter	Type	Description
application_id	String	Application ID. Its prefix is **app-**.
display	**DisplayDto** object	Display information of an application.
application_type	String	Application type.

Table 4-343 DisplayDto

Parameter	Type	Description
description	String	Application description.
display_name	String	Application display name.
icon	String	Application icon.

Table 4-344 PageInfoDto

Parameter	Type	Description
next_marker	String	If present, more output is available than that included in the current response. To get the next part of the output, use this value in the request parameter in a subsequent call to the same API. You should repeat calling until the **next_marker** parameter is null in a response.

Parameter	Type	Description
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-345 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-346 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing preset application templates in the application directory

```
GET https://{hostname}/v1/catalog/applications
```

Example Response

Status code: 200

Successful

```
{
  "applications" : [ {
    "application_id" : "app-e7f300xxxxx",
    "display" : {
      "description" : "description",
      "display_name" : "custom-saml"
    }
  } ],
```



```
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.6.4 Listing Application Providers

Function

This API is used to list application providers. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/application-providers

Table 4-347 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request.
marker	No	String	Pagination marker.

Request Parameters

Table 4-348 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-349 Parameters in the response body

Parameter	Type	Description
application_providers	Array of **ApplicationProviderDto** objects	List of application providers.
page_info	**PageInfoDto** object	Pagination information.

Table 4-350 ApplicationProviderDto

Parameter	Type	Description
application_provider_urn	String	Application provider URN.
display_data	**DisplayDataDto** object	Display information of an application provider.
federation_protocol	String	Supported protocols.
application_provider_id	String	Unique ID of an application provider.

Table 4-351 DisplayDataDto

Parameter	Type	Description
description	String	Description of an application provider.

Parameter	Type	Description
display_name	String	Display name of an application provider.
icon_url	String	Icon of an application provider.

Table 4-352 PageInfoDto

Parameter	Type	Description
next_marker	String	If present, more output is available than that included in the current response. To get the next part of the output, use this value in the request parameter in a subsequent call to the same API. You should repeat calling until the **next_marker** parameter is null in a response.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-353 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-354 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing application providers

```
GET https://{hostname}/v1/application-providers
```

Example Response

Status code: 200

Successful

```
{
  "application_providers" : [ {
    "application_provider_id" : "app-xxxxxx",
    "application_provider_urn" : "IdentityCenter::x-xxxxx",
    "display_data" : {
      "description" : "description",
      "display_name" : "custom-saml"
    },
    "federation_protocol" : "SAML"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.6.5 Listing Application Templates

Function

This API is used to list application templates. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/application-templates

Table 4-355 Query parameters

Parameter	Mandatory	Type	Description
application_id	Yes	String	Application ID. Its prefix is **app-**.

Request Parameters

Table 4-356 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-357 Parameters in the response body

Parameter	Type	Description
application_templates	Array of **ApplicationTemplateDto** objects	List of application templates.

Table 4-358 ApplicationTemplateDto

Parameter	Type	Description
application	**ApplicationTemplateDisplayDto** object	Display information of an application template.
response_config	**ResponseConfigDto** object	Application attribute configuration.
response_schema_config	**ResponseSchemaConfigDto** object	Mapping configuration of application attributes.
sso_protocol	String	Supported protocols.
security_config	**SecurityConfigDto** object	Certificate configuration.

Parameter	Type	Description
service_provider_config	**ServiceProvider-ConfigDto** object	Service provider configuration.
template_id	String	Unique ID of an application template.
template_version	String	Application template version.

Table 4-359 ApplicationTemplateDisplayDto

Parameter	Type	Description
application_id	String	Application ID. Its prefix is **app-**.
display	**DisplayDto** object	Display information of an application.
application_type	String	Application type.

Table 4-360 DisplayDto

Parameter	Type	Description
description	String	Application description.
display_name	String	Application display name.
icon	String	Application icon.

Table 4-361 ResponseConfigDto

Parameter	Type	Description
properties	Map<String,**ResponseSourceDetailsDto**>	Additional configuration for attribute mapping.
subject	**ResponseSourceDetailsDto** object	Subject attribute mapping configuration.
relay_state	String	Relay state.
ttl	String	Session expiration time.

Table 4-362 ResponseSourceDetailsDto

Parameter	Type	Description
source	Array of strings	Attribute mapping value.

Table 4-363 ResponseSchemaConfigDto

Parameter	Type	Description
properties	Map<String,**ResponseSchemaPropertiesDetailsDto**>	Additional schema configuration for attribute mapping.
subject	**ResponseSchemaSubjectDetailsDto** object	Schema configuration for subject attribute mapping.
supported_name_id_formats	Array of strings	Subject NameID format supported by an application.

Table 4-364 ResponseSchemaPropertiesDetailsDto

Parameter	Type	Description
attr_name_format	String	Additional attribute format.
include	String	Whether additional attributes are included.

Table 4-365 ResponseSchemaSubjectDetailsDto

Parameter	Type	Description
name_id_format	String	NameID format.
include	String	Whether NameID is included.

Table 4-366 SecurityConfigDto

Parameter	Type	Description
ttl	String	Certificate expiration time.

Table 4-367 ServiceProviderConfigDto

Parameter	Type	Description
audience	String	SAML audience.
require_request_signature	Boolean	Whether a signature is required.

Parameter	Type	Description
consumers	Array of ConsumersDto objects	SAML response recipient.
start_url	String	Application startup URL.

Table 4-368 ConsumersDto

Parameter	Type	Description
binding	String	SAML transmission protocol.
default_value	Boolean	Whether it is the default recipient.
location	String	SAML ACS URL.

Status code: 400

Table 4-369 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-370 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing application templates


```
GET https://{hostname}/v1/application-templates
```

Example Response

Status code: 200

Successful


```
{
  "application_templates" : [ {
    "application" : {
      "application_id" : "app-ff1258a63a4a263f",
      "display" : {
        "description" : "Custom SAML 2.0 application",
        "display_name" : "Custom SAML 2.0 application",
        "icon" : ""
      },
      "application_type" : ""
    },
    "response_config" : {
      "properties" : { },
      "subject" : null,
      "relay_state" : null,
      "ttl" : "PT1H"
    },
    "response_schema_config" : {
      "properties" : { },
      "subject" : null,
      "supported_name_id_formats" : null
    },
    "sso_protocol" : "SAML",
    "security_config" : {
      "ttl" : null
    },
    "service_provider_config" : {
      "audience" : null,
      "require_request_signature" : false,
      "consumers" : null,
      "start_url" : null
    },
    "template_id" : "tpl-88f215b39bfc7575",
    "template_version" : "1"
  } ]
}
```


Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.6.6 Querying Configurations of Application Assignment Attributes

Function

This API is used to query configurations of application assignment attributes to assign application access permissions to users or user groups. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/applications/{application_instance_id}/assignments-configuration

Table 4-371 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-372 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-373 Parameters in the response body

Parameter	Type	Description
assignment_required	Boolean	Whether an application needs to be assigned.

Status code: 400

Table 4-374 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-375 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-376 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Querying configurations of application allocation attributes

```
GET https://{hostname}/v1/instances/{instance_id}/applications/{application_instance_id}/assignments-configuration
```

Example Response

Status code: 200

Successful


```
{
  "assignment_required" : true
}
```

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.6.7 Updating Display Information of an Application Instance

Function

This API is used to update the display information of an application instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/display-data

Table 4-377 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-378 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-379 Parameters in the request body

Parameter	Mandatory	Type	Description
description	Yes	String	Application description.
display_name	Yes	String	Application display name.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-380 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-381 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted error message.

Example Request

Updating display information of an application instance

```
PUT https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}/display-data

{
  "display_name" : "Custom SAML 2.0 application",
  "description" : "test"
}
```

Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.6.8 Uploading an Application Instance Metadata File

Function

This API is used to upload an application instance metadata file. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/application-instances/{application_instance_id}/metadata

Table 4-382 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-383 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-384 Parameters in the request body

Parameter	Mandatory	Type	Description
metadata	Yes	String	Metadata file.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-385 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-386 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Uploading an application instance metadata file

```
POST https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}/metadata

{
  "metadata" : "metadata text"
}
```

Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.6.9 Updating Application Attribute Configurations

Function

This API is used to update application attribute configurations, including the attribute mapping, relay state, and session expiration time in the application. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/response-configuration

Table 4-387 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-388 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-389 Parameters in the request body

Parameter	Mandatory	Type	Description
response_config	Yes	**ResponseConfigDto** object	Application attribute configuration.

Table 4-390 ResponseConfigDto

Parameter	Mandatory	Type	Description
properties	No	Map<String,**ResponseSourceDetailsDto**>	Additional configuration for attribute mapping.
subject	No	**ResponseSourceDetailsDto** object	Subject attribute mapping configuration.
relay_state	No	String	Relay state.
ttl	Yes	String	Session expiration time.

Table 4-391 ResponseSourceDetailsDto

Parameter	Mandatory	Type	Description
source	Yes	Array of strings	Attribute mapping value.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-392 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-393 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-394 Parameters in the response body

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

Parameter	Type	Description
request_id	String	Unique ID of a request.

Example Request

Updating application attribute configurations, including the attribute mapping, relay state, and session expiration time in the application

```
PUT https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}/response-configuration

{
  "response_config" : {
    "properties" : {
      "username" : {
        "source" : [ "${user:familyName}" ]
      }
    },
    "subject" : {
      "source" : [ "${user:email}" ]
    },
    "relay_state" : null,
    "ttl" : "PT1H"
  }
}
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.6.10 Updating Schema Attribute Mapping Configurations of an Application

Function

This API is used to update schema attribute mapping configurations of an application to support Subject attribute mapping and the Subject NameID format

in SAML assertions. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/response-schema-configuration

Table 4-395 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-396 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-397 Parameters in the request body

Parameter	Mandatory	Type	Description
response_schema_config	Yes	**ResponseSchemaConfigDto** object	Configuration for application schema attribute mapping.

Table 4-398 ResponseSchemaConfigDto

Parameter	Mandatory	Type	Description
properties	No	Map<String,**ResponseSchemaPropertiesDetailsDto**>	Additional schema configuration for attribute mapping.

Parameter	Mandatory	Type	Description
subject	Yes	ResponseSchemaSubjectDetailsDto object	Schema configuration for subject attribute mapping.
supported_name_id_formats	No	Array of strings	Subject NameID format supported by an application.

Table 4-399 ResponseSchemaPropertiesDetailsDto

Parameter	Mandatory	Type	Description
attr_name_format	Yes	String	Additional attribute format.
include	Yes	String	Whether additional attributes are included.

Table 4-400 ResponseSchemaSubjectDetailsDto

Parameter	Mandatory	Type	Description
name_id_format	Yes	String	NameID format.
include	Yes	String	Whether NameID is included.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-401 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-402 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-403 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Updating schema attribute mapping configurations of an application to support Subject attribute mapping and the Subject NameID format in SAML assertions

```
PUT https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}/response-schema-configuration

{
  "response_schema_config" : {
    "properties" : { },
    "subject" : {
      "name_id_format" : "nameid-format:unspecified",
      "include" : "REQUIRED"
    },
    "supported_name_id_formats" : [ "nameid-format:unspecified" ]
  }
}
```

Example Response

None

Status Codes

Status Code	Description
200	Successful.

Status Code	Description
400	Bad request.
403	Forbidden.
404	Not found.

Error Codes

For details, see **Error Codes**.

4.6.11 Updating Service Provider Configurations for an Application Instance

Function

This API is used to update service provider configurations for an application instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/service-provider-configuration

Table 4-404 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-405 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-406 Parameters in the request body

Parameter	Mandatory	Type	Description
service_provider_config	Yes	**ServiceProviderConfigDto** object	Service provider configuration.

Table 4-407 ServiceProviderConfigDto

Parameter	Mandatory	Type	Description
audience	Yes	String	SAML audience.
require_request_signature	No	Boolean	Whether a signature is required.
consumers	Yes	Array of **ConsumersDto** objects	SAML response recipient.
start_url	No	String	Application startup URL.

Table 4-408 ConsumersDto

Parameter	Mandatory	Type	Description
binding	Yes	String	SAML transmission protocol.
default_value	Yes	Boolean	Whether it is the default recipient.
location	Yes	String	SAML ACS URL.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-409 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-410 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-411 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Updating service provider configurations of an application instance

```
PUT https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}/service-provider-configuration

{
  "service_provider_config" : {
    "audience" : "https://xxx.example.com",
    "require_request_signature" : false,
    "consumers" : [ {
      "location" : "https://xxx.example.com/acs",
      "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
      "default_value" : true
    } ],
    "start_url" : "https://xxx.example.com/acs"
  }
}
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.6.12 Updating the Application Instance Status

Function

This API is used to update the application instance status. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/status

Table 4-412 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-413 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-414 Parameters in the request body

Parameter	Mandatory	Type	Description
status	Yes	String	Application status.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-415 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-416 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-417 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Updating the application instance status

```
PUT https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}/status

{
  "status" : "ENABLED"
}
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.6.13 Updating Certificate Configurations of an Application Instance

Function

This API is used to update certificate configurations of an application instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/security-configuration

Table 4-418 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-419 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-420 Parameters in the request body

Parameter	Mandatory	Type	Description
security_config	Yes	**SecurityConfigDto** object	Certificate configuration.

Table 4-421 SecurityConfigDto

Parameter	Mandatory	Type	Description
ttl	Yes	String	Certificate expiration time.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-422 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-423 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Updating certificate configurations of an application instance

```
PUT https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}/security-configuration

{
  "security_config" : {
    "ttl" : "P9M"
  }
}
```


Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.6.14 Querying Application Details

Function

This API is used to query application details. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/applications/{application_instance_id}

Table 4-424 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-425 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-426 Parameters in the response body

Parameter	Type	Description
application_urn	String	Application URN.
application_provider_urn	String	Application provider URN.
assignment_config	**AssignmentConfigDto** object	Whether an application needs to be assigned.
created_date	Long	Creation time.
description	String	Application description.
instance_urn	String	URN of an IAM Identity Center instance.
name	String	Application display name.
portal_options	**PortalOptionsDto** object	Portal option settings.
status	String	Status.
application_account	String	Huawei Cloud account.

Table 4-427 AssignmentConfigDto

Parameter	Type	Description
assignment_required	Boolean	Whether an application needs to be assigned.

Table 4-428 PortalOptionsDto

Parameter	Type	Description
visible	Boolean	Whether an application is visible on the user portal.
visibility	String	Application visibility on the portal.
sign_in_options	**SignInOptionsDto** object	Portal login options.

Table 4-429 SignInOptionsDto

Parameter	Type	Description
origin	String	Method of redirecting to an application from IAM Identity Center.
application_url	String	URL for receiving application authentication requests.

Status code: 400

Table 4-430 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-431 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-432 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Querying application details

```
GET https://{hostname}/v1/instances/{instance_id}/applications/{application_instance_id}
```

Example Response

Status code: 200

Successful

```
{
  "application_urn" : "IdentityCenter::8c1eef3a241945f69c3dxxxxx:application:ins-36218e5b4c2c0504/apl-e7f30081e5ff428c",
  "application_provider_urn" : "IdentityCenter:::applicationProvider:custom-saml",
  "assignment_config" : {
    "assignment_required" : true
  },
  "created_date" : 1752041671967,
  "description" : "ApplicationStartUrl",
  "instance_urn" : "IdentityCenter::8c1eef3a241945f69c3d3axxxxx:instance:ins-36218e5b4c2c0504",
  "name" : "ApplicationStartUrl",
  "portal_options" : {
    "visible" : true,
    "visibility" : "ENABLED",
    "sign_in_options" : {
      "origin" : "IDENTITY_CENTER",
      "application_url" : ""
    }
  },
  "status" : "ENABLED",
  "application_account" : "8c1eef3a241945f69c3d3a6b0252e783"
}
```

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.6.15 Listing Applications

Function

This API is used to list applications. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/applications

Table 4-433 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Table 4-434 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request.
marker	No	String	Pagination marker.

Request Parameters

Table 4-435 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-436 Parameters in the response body

Parameter	Type	Description
applications	Array of **ApplicationDto** objects	Application list.
page_info	**PageInfoDto** object	Pagination information.

Table 4-437 ApplicationDto

Parameter	Type	Description
application_urn	String	Application URN.
application_provider_urn	String	Application provider URN.
assignment_config	**AssignmentConfigDto** object	Whether an application needs to be assigned.
created_date	Long	Time when an application is created.
description	String	Application description.
instance_urn	String	URN of an IAM Identity Center instance.
name	String	Application display name.
portal_options	**PortalOptionsDto** object	Portal option settings.
status	String	Application status.
application_account	String	Huawei Cloud account.

Table 4-438 AssignmentConfigDto

Parameter	Type	Description
assignment_required	Boolean	Whether an application needs to be assigned.

Table 4-439 PortalOptionsDto

Parameter	Type	Description
visible	Boolean	Whether an application is visible on the user portal.
visibility	String	Application visibility on the portal.
sign_in_options	**SignInOptionsDto** object	Portal login options.

Table 4-440 SignInOptionsDto

Parameter	Type	Description
origin	String	Method of redirecting to an application from IAM Identity Center.
application_url	String	URL for receiving application authentication requests.

Table 4-441 PageInfoDto

Parameter	Type	Description
next_marker	String	If present, more output is available than that included in the current response. To get the next part of the output, use this value in the request parameter in a subsequent call to the same API. You should repeat calling until the **next_marker** parameter is null in a response.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-442 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-443 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-444 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Listing applications

```
GET https://{hostname}/v1/instances/{instance_id}/applications
```

Example Response

Status code: 200

Successful

```
{
  "applications" : [ {
    "application_urn" : "IdentityCenter::8c1eef3a241945f69c3d3a6b0xxxxx:application:ins-36218e5b4c2c0504/apl-e7f30081e5ff428c",
    "application_provider_urn" : "IdentityCenter:::applicationProvider:custom-saml",
    "assignment_config" : {
      "assignment_required" : true
    },
    "created_date" : 1752041671967,
    "description" : "ApplicationStartUrl",
    "instance_urn" : "IdentityCenter::8c1eef3a241945f69c3d3a6bxxxxx:instance:ins-36218e5b4c2c0504",
    "name" : "ApplicationStartUrl",
    "portal_options" : {
      "visible" : true,
      "visibility" : "ENABLED",
      "sign_in_options" : {
        "origin" : "IDENTITY_CENTER",
        "application_url" : ""
```



```
    }
   },
   "status" : "ENABLED",
   "application_account" : "8c1eef3a241945f69c3d3a6b0252e783"
  } ],
  "page_info" : {
   "next_marker" : null,
   "current_count" : 1
  }
}
```


Status Codes

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

Error Codes

For details, see **Error Codes**.

4.6.16 Querying Application Instance Details

Function

This API is used to query application instance details. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/application-instances/{application_instance_id}

Table 4-445 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-446 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-447 Parameters in the response body

Parameter	Type	Description
application_instance	**ApplicationInstanceDto** object	Application instance.

Table 4-448 ApplicationInstanceDto

Parameter	Type	Description
active_certificate	**CertificateDto** object	Activated certificates.
display	**DisplayDto** object	Display information of an application.
identity_provider_config	**IdentityProviderConfigDto** object	Identity provider configuration.
application_instance_id	String	Unique ID of an application instance.
name	String	Application UUID.
visible	Boolean	Whether an application is visible on the user portal.
response_config	**ResponseConfigDto** object	Application attribute configuration.
response_schema_config	**ResponseSchemaConfigDto** object	Configuration for application schema attribute mapping.
security_config	**SecurityConfigDto** object	Certificate configuration.

Parameter	Type	Description
status	String	Application instance status.
template	**ApplicationTemplateDto** object	Information about the template that an application depends on.
service_provider_config	**ServiceProvider-ConfigDto** object	Service provider configuration.
client_id	String	OIDC client ID.
end_user_visible	Boolean	Visible to users or not.
managed_account	String	Account ID of a group member.

Table 4-449 CertificateDto

Parameter	Type	Description
algorithm	String	Certificate generation algorithm.
certificate	String	Application certificate.
certificate_id	String	Application certificate ID.
expiry_date	Long	Certificate expiration time.
status	String	Certificate status.
key_size	String	Key size.
issue_date	Long	Certificate generation time.

Table 4-450 IdentityProviderConfigDto

Parameter	Type	Description
issuer_url	String	Identity provider issuer.
metadata_url	String	Identity provider metadata.
remote_login_url	String	Remote login link of an identity provider.
remote_logout_url	String	Remote logout link of an identity provider.

Table 4-451 ApplicationTemplateDto

Parameter	Type	Description
application	**ApplicationTemplateDisplayDto** object	Display information of an application template.
response_config	**ResponseConfigDto** object	Application attribute configuration.
response_schema_config	**ResponseSchemaConfigDto** object	Mapping configuration of application attributes.
sso_protocol	String	Supported protocols.
security_config	**SecurityConfigDto** object	Certificate configuration.
service_provider_config	**ServiceProviderConfigDto** object	Service provider configuration.
template_id	String	Unique ID of an application template.
template_version	String	Application template version.

Table 4-452 ApplicationTemplateDisplayDto

Parameter	Type	Description
application_id	String	Application ID. Its prefix is **app-**.
display	**DisplayDto** object	Display information of an application.
application_type	String	Application type.

Table 4-453 DisplayDto

Parameter	Type	Description
description	String	Application description.
display_name	String	Application display name.
icon	String	Application icon.

Table 4-454 ResponseConfigDto

Parameter	Type	Description
properties	Map<String,**ResponseSourceDetailsDto**>	Additional configuration for attribute mapping.
subject	**ResponseSourceDetailsDto** object	Subject attribute mapping configuration.
relay_state	String	Relay state.
ttl	String	Session expiration time.

Table 4-455 ResponseSourceDetailsDto

Parameter	Type	Description
source	Array of strings	Attribute mapping value.

Table 4-456 ResponseSchemaConfigDto

Parameter	Type	Description
properties	Map<String,**ResponseSchemaPropertiesDetailsDto**>	Additional schema configuration for attribute mapping.
subject	**ResponseSchemaSubjectDetailsD-to** object	Schema configuration for subject attribute mapping.
supported_name_id_formats	Array of strings	Subject NameID format supported by an application.

Table 4-457 ResponseSchemaPropertiesDetailsDto

Parameter	Type	Description
attr_name_format	String	Additional attribute format.
include	String	Whether additional attributes are included.

Table 4-458 ResponseSchemaSubjectDetailsDto

Parameter	Type	Description
name_id_format	String	NameID format.
include	String	Whether NameID is included.

Table 4-459 SecurityConfigDto

Parameter	Type	Description
ttl	String	Certificate expiration time.

Table 4-460 ServiceProviderConfigDto

Parameter	Type	Description
audience	String	SAML audience.
require_request_signature	Boolean	Whether a signature is required.
consumers	Array of **ConsumersDto** objects	SAML response recipient.
start_url	String	Application startup URL.

Table 4-461 ConsumersDto

Parameter	Type	Description
binding	String	SAML transmission protocol.
default_value	Boolean	Whether it is the default recipient.
location	String	SAML ACS URL.

Status code: 400

Table 4-462 Parameters in the response body

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

Parameter	Type	Description
request_id	String	Unique ID of a request.

Status code: 403

Table 4-463 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-464 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Querying application instance details

```
GET https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}
```

Example Response

Status code: 200

Successful

```
{
  "application_instance" : {
    "active_certificate" : {
      "algorithm" : "SHA256withRSA",
      "certificate" : "certificate text",
      "certificate_id" : "cer-ea56cf20-4ec3-445a-883f-eb70f35fe7d1",
      "expiry_date" : 1911427200000,
      "status" : "ACTIVE",
      "key_size" : "3072",
      "issue_date" : 1753695145064
```



```
  },
  "display" : {
    "description" : "teststsfs",
    "display_name" : "Custom SAML 2.0 application",
    "icon" : ""
  },
  "identity_provider_config" : {
    "issuer_url" : "https://idcenter.ulanqab.huawei.com/v1/saml/assertion/
OGMxZWVmM2EyNDE5NDVmNjljM2QzYTZiMDI1MmU3ODNfZC05NDE0MDdiNGIzX2FwcC1pbnMtYTAzM2
M5MDcwMTZhNTlhZQ==",
    "metadata_url" : "https://idcenter.ulanqab.huawei.com/v1/saml/metadata/
OGMxZWVmM2EyNDE5NDVmNjljM2QzYTZiMDI1MmU3ODNfZC05NDE0MDdiNGIzX2FwcC1pbnMtYTAzM2
M5MDcwMTZhNTlhZQ==",
    "remote_login_url" : "https://idcenter.ulanqab.huawei.com/v1/saml/assertion/
OGMxZWVmM2EyNDE5NDVmNjljM2QzYTZiMDI1MmU3ODNfZC05NDE0MDdiNGIzX2FwcC1pbnMtYTAzM2
M5MDcwMTZhNTlhZQ==",
    "remote_logout_url" : "https://idcenter.ulanqab.huawei.com/v1/saml/logout/
OGMxZWVmM2EyNDE5NDVmNjljM2QzYTZiMDI1MmU3ODNfZC05NDE0MDdiNGIzX2FwcC1pbnMtYTAzM2
M5MDcwMTZhNTlhZQ=="
  },
  "application_instance_id" : "app-ins-a033c907016a59ae",
  "name" : "a689ebed-1b68-44b0-af97-0be880c30127",
  "visible" : true,
  "response_config" : {
    "properties" : { },
    "subject" : null,
    "relay_state" : null,
    "ttl" : "PT1H"
  },
  "response_schema_config" : {
    "properties" : { },
    "subject" : null,
    "supported_name_id_formats" : null
  },
  "security_config" : {
    "ttl" : "P5Y"
  },
  "status" : "ENABLED",
  "template" : {
    "application" : {
      "application_id" : "app-ff1258a63a4a263f",
      "display" : {
        "description" : "Custom SAML 2.0 application",
        "display_name" : "Custom SAML 2.0 application",
        "icon" : ""
      },
      "application_type" : ""
    },
    "response_config" : {
      "properties" : { },
      "subject" : null,
      "relay_state" : null,
      "ttl" : "PT1H"
    },
    "response_schema_config" : {
      "properties" : { },
      "subject" : null,
      "supported_name_id_formats" : null
    },
    "sso_protocol" : "SAML",
    "security_config" : {
      "ttl" : null
    },
    "service_provider_config" : {
      "audience" : null,
      "require_request_signature" : false,
      "consumers" : null,
      "start_url" : null
    },
```



```
    "template_id" : "tpl-88f215b39bfc7575",
    "template_version" : "1"
   },
   "service_provider_config" : {
    "audience" : "https://console.ulanqab.huawei.com/identitycenter/?region=cn-north-7&locale=zh-cn#/
application/add/app-ins-a033c907016a59ae",
    "require_request_signature" : false,
    "consumers" : [ {
     "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
     "default_value" : true,
     "location" : "https://console.ulanqab.huawei.com/identitycenter/?region=cn-north-7&locale=zh-cn#/
application/add/app-ins-a033c907016a59ae"
    } ],
    "start_url" : null
   },
   "client_id" : null,
   "end_user_visible" : null,
   "managed_account" : "8c1eef3a241945f69c3d3a6b0252e783"
  }
}
```


Status Codes

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

Error Codes

For details, see **Error Codes**.

4.6.17 Deleting an Application Instance

Function

This API is used to delete an application instance. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/instances/{instance_id}/application-instances/{application_instance_id}

Table 4-465 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Parameter	Mandatory	Type	Description
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-466 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-467 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-468 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-469 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Deleting an application instance

```
DELETE https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.6.18 Querying Application Provider Details

Function

This API is used to query application provider details. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/application-providers/{application_provider_id}

Table 4-470 Path parameters

Parameter	Mandatory	Type	Description
application_provider_id	Yes	String	Application provider ID.

Request Parameters

Table 4-471 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-472 Parameters in the response body

Parameter	Type	Description
application_provider_urn	String	Application provider URN.
display_data	**DisplayDataDto** object	Display information of an application provider.
federation_protocol	String	Supported protocols.
application_provider_id	String	Unique ID of an application provider.

Table 4-473 DisplayDataDto

Parameter	Type	Description
description	String	Description of an application provider.
display_name	String	Display name of an application provider.
icon_url	String	Icon of an application provider.

Status code: 400

Table 4-474 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-475 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-476 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Querying application provider details

```
GET https://{hostname}/v1/application-providers/{application_provider_id}
```

Example Response

Status code: 200

Successful.

```
{
  "application_provider_id" : "app-xxxxxxx",
```

```
  "application_provider_urn" : "IdentityCenter::x-xxxxx",
  "display_data" : {
    "description" : "description",
    "display_name" : "custom-saml"
  },
  "federation_protocol" : "SAML"
}
```

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.6.19 Listing Associations Between an Application Instance and a User or User Group

Function

This API is used to list associations between an application instance and a user or user group. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/application-instances/{application_instance_id}/profiles

Table 4-477 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-478 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-479 Parameters in the response body

Parameter	Type	Description
applicationProfiles	Array of **ApplicationProfileDto** objects	Application profile.

Table 4-480 ApplicationProfileDto

Parameter	Type	Description
name	String	Association name. The default value is **Default**.
status	String	Association status. The default value is **ENABLED**.
profile_id	String	ID of the association between a principal and an application.

Status code: 400

Table 4-481 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-482 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-483 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Listing associations between an application instance and a user or user group

```
GET https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}/profiles
```

Example Response

Status code: 200

Successful

```
{
  "application_profiles" : [ {
    "name" : "Default",
    "status" : "ENABLED",
    "profile_id" : "p-dc6434b56c4e5221"
  } ]
}
```

Status Codes

Status Code	Description
200	Successful.

Status Code	Description
400	Bad request.
403	Forbidden.
404	Not found.

Error Codes

For details, see **Error Codes**.

4.6.20 Deleting the Association Between an Application Instance and a User or User Group

Function

This API is used to delete the association between an application instance and a user or user group. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/instances/{instance_id}/application-instances/{application_instance_id}/profiles/{profile_id}

Table 4-484 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.
profile_id	Yes	String	ID of the association between an application instance and a user or user group.

Request Parameters

Table 4-485 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-486 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-487 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-488 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Deleting the association between an application instance and a user or user group

```
DELETE https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}/profiles/{profile_id}
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.7 Application Assignment Management

4.7.1 Listing Users or User Groups Assigned to an Application

Function

This API is used to list users or user groups assigned to an application. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/applications/{application_instance_id}/assignments

Table 4-489 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Table 4-490 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request.
marker	No	String	Pagination marker.

Request Parameters

Table 4-491 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-492 Parameters in the response body

Parameter	Type	Description
application_assignments	Array of **ApplicationAssignmentDto** objects	List of users or user groups assigned to an application.

Parameter	Type	Description
page_info	**PageInfoDto** object	Pagination information.

Table 4-493 ApplicationAssignmentDto

Parameter	Type	Description
application_urn	String	Application URN.
principal_id	String	Principal ID.
principal_type	String	Principal type.

Table 4-494 PageInfoDto

Parameter	Type	Description
next_marker	String	If present, more output is available than that included in the current response. To get the next part of the output, use this value in the request parameter in a subsequent call to the same API. You should repeat calling until the **next_marker** parameter is null in a response.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-495 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-496 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing users or user groups assigned to an application

```
GET https://{hostname}/v1/instances/{instance_id}/applications/{application_instance_id}/assignments
```

Example Response

Status code: 200

Successful

```
{
  "application_assignments" : [ {
    "application_urn" : "IdentityCenter::8c1eef3a241945f69c3d3a6bxxxxxx:application:ins-36218e5b4c2xxxx/apl-83142f08178ce349",
    "principal_id" : "4b969bc6-e8ed-47ce-b62b-936319xxxx1",
    "principal_type" : "USER"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.7.2 Assigning a User or User Group to an Application

Function

This API is used to assign users or user groups to an application. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/applications/{application_instance_id}/assignments/create

Table 4-497 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-498 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-499 Parameters in the request body

Parameter	Mandatory	Type	Description
principal_id	Yes	String	Principal ID.
principal_type	Yes	String	Principal type.

Response Parameters

Status code: 201

Successful

Status code: 400

Table 4-500 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-501 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 409

Table 4-502 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Assigning users or user groups to an application

```
POST https://{hostname}/v1/instances/{instance_id}/applications/{application_instance_id}/assignments/create

{
  "principal_id" : "b2d3de5e-6689-4e50-8faa-c6dd00eca943",
  "principal_type" : "USER"
}
```


Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.7.3 Deleting Users or User Groups Assigned to an Application

Function

This API is used to delete users or user groups assigned to an application. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/applications/{application_instance_id}/assignments/delete

Table 4-503 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-504 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-505 Parameters in the request body

Parameter	Mandatory	Type	Description
principal_id	Yes	String	Principal ID.
principal_type	Yes	String	Principal type.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-506 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-507 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-508 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Deleting users or user groups assigned to an application

```
POST https://{hostname}/v1/instances/{instance_id}/applications/{application_instance_id}/assignments/delete

{
  "principal_id" : "b2d3de5e-6689-4e50-8faa-c6dd00eca943",
  "principal_type" : "USER"
}
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.7.4 Listing Applications Associated with a User or User Group

Function

This API is used to list applications associated with a user or user group. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/application-assignments-for-principals

Table 4-509 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Table 4-510 Query parameters

Parameter	Mandatory	Type	Description
principal_id	Yes	String	Globally unique ID of a principal.
principal_type	Yes	String	Principal type. The value can be **USER** or **GROUP**.
limit	No	Integer	Maximum number of results returned for each request.
marker	No	String	Pagination marker.

Request Parameters

Table 4-511 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-512 Parameters in the response body

Parameter	Type	Description
application_assignments	Array of **ApplicationAssignmentDto** objects	Principal assigned with an application.
page_info	**PageInfoDto** object	Pagination information.

Table 4-513 ApplicationAssignmentDto

Parameter	Type	Description
application_urn	String	Application URN.
principal_id	String	Principal ID.
principal_type	String	Principal type.

Table 4-514 PageInfoDto

Parameter	Type	Description
next_marker	String	If present, more output is available than that included in the current response. To get the next part of the output, use this value in the request parameter in a subsequent call to the same API. You should repeat calling until the **next_marker** parameter is null in a response.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-515 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-516 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing applications associated with a user or user group

```
GET https://{hostname}/v1/instances/{instance_id}/application-assignments-for-principals
```

Example Response

Status code: 200

Successful

```
{
  "application_assignments" : [ {
    "application_urn" : "IdentityCenter::8c1eef3a241945f69c3d3a6b0xxxxx:application:ins-36218e5b4cxxxx/
apl-83142f08178ce359",
    "principal_id" : "4b969bc6-e8ed-47ce-b62b-936319e2bcb1",
    "principal_type" : "USER"
  }, {
    "application_urn" : "IdentityCenter::8c1eef3a241945f69c3d3a6b02xxx:application:ins-36218e5b4c2cxxx/
apl-83142f08178ce349",
    "principal_id" : "4b969bc6-e8ed-47ce-b62b-936319e2bcb1",
    "principal_type" : "USER"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 2
  }
}
```


Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.8 Application Certificate Management

4.8.1 Activating Application Instance Certificates

Function

This API is used to activate application instance certificates to implement certificate rotation. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/certificates/{certificate_id}

Table 4-517 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.
certificate_id	Yes	String	Globally unique ID of an application certificate.

Request Parameters

Table 4-518 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-519 Parameters in the response body

Parameter	Type	Description
application_instance_certificate	**CertificateDto** object	Application certificate.

Table 4-520 CertificateDto

Parameter	Type	Description
algorithm	String	Certificate generation algorithm.
certificate	String	Application certificate.
certificate_id	String	Application certificate ID.
expiry_date	Long	Certificate expiration time.
status	String	Certificate status.
key_size	String	Key size.
issue_date	Long	Certificate generation time.

Status code: 400

Table 4-521 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-522 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-523 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Activating application instance certificates to implement certificate rotation

```
PUT https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}/
certificates/{certificate_id}
```

Example Response

Status code: 200

Successful

```
{
  "application_instance_certificate" : {
    "algorithm" : "SHA256withRSA",
    "certificate" : "certificate text",
    "certificate_id" : "cer-5c81c5ce-c16c-4a5d-8e55-f491f2239f1a",
    "expiry_date" : 1767916800000,
```



```
    "status" : "ACTIVE",
    "key_size" : "3072",
    "issue_date" : 1752048619976
  }
}
```

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.8.2 Deleting an Application Instance Certificate

Function

This API is used to delete an application instance certificate. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/instances/{instance_id}/application-instances/{application_instance_id}/certificates/{certificate_id}

Table 4-524 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.
certificate_id	Yes	String	Globally unique ID of an application certificate.

Request Parameters

Table 4-525 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-526 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-527 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-528 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Deleting an application instance certificate

```
DELETE https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}/certificates/{certificate_id}
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.8.3 Creating an Application Instance Certificate

Function

This API is used to create an application instance certificate. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/application-instances/{application_instance_id}/certificates

Table 4-529 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Request Parameters

Table 4-530 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 201

Table 4-531 Parameters in the response body

Parameter	Type	Description
application_instance_certificate	**CertificateDto** object	Application certificate.

Table 4-532 CertificateDto

Parameter	Type	Description
algorithm	String	Certificate generation algorithm.
certificate	String	Application certificate.
certificate_id	String	Application certificate ID.
expiry_date	Long	Certificate expiration time.
status	String	Certificate status.
key_size	String	Key size.
issue_date	Long	Certificate generation time.

Status code: 400

Table 4-533 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-534 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 409

Table 4-535 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Creating an application instance certificate

```
POST https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}/certificates
```

Example Response

Status code: 201

Successful.


```
{
  "application_instance_certificate" : {
    "algorithm" : "SHA256withRSA",
    "certificate" : "-----BEGIN CERTIFICATE-----\r\nMIIEyzCCAzOgAwI*******lQxBvg==\r\n-----END
CERTIFICATE-----",
    "certificate_id" : "cer-4d47a100-0144-492d-8aa5-9460c6aadc55",
    "expiry_date" : 1912291200000,
    "status" : "INACTIVE",
    "key_size" : "3072",
    "issue_date" : 1754548061000
  }
}
```


Status Codes

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

Error Codes

For details, see **Error Codes**.

4.8.4 Listing Application Instance Certificates

Function

This API is used to list application instance certificates. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/application-instances/{application_instance_id}/certificates

Table 4-536 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.
application_instance_id	Yes	String	Application instance ID. Its prefix is **app-ins-**.

Table 4-537 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request.
marker	No	String	Pagination marker.

Request Parameters

Table 4-538 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-539 Parameters in the response body

Parameter	Type	Description
application_instance_certificates	Array of **CertificateDto** objects	List of application certificates.
page_info	**PageInfoDto** object	Pagination information.

Table 4-540 CertificateDto

Parameter	Type	Description
algorithm	String	Certificate generation algorithm.
certificate	String	Application certificate.
certificate_id	String	Application certificate ID.
expiry_date	Long	Certificate expiration time.
status	String	Certificate status.

Parameter	Type	Description
key_size	String	Key size.
issue_date	Long	Certificate generation time.

Table 4-541 PageInfoDto

Parameter	Type	Description
next_marker	String	If present, more output is available than that included in the current response. To get the next part of the output, use this value in the request parameter in a subsequent call to the same API. You should repeat calling until the **next_marker** parameter is null in a response.
current_count	Integer	Number of items returned on this page.

Status code: 400

Table 4-542 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-543 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing application instance certificates

```
GET https://{hostname}/v1/instances/{instance_id}/application-instances/{application_instance_id}/
certificates
```

Example Response

Status code: 200

Successful.


```
{
  "application_instance_certificates" : [ {
    "algorithm" : "SHA256withRSA",
    "certificate" : "certificate text",
    "certificate_id" : "cer-5c81c5ce-c16c-4a5d-8e55-f491f2239f1a",
    "expiry_date" : 1767916800000,
    "status" : "ACTIVE",
    "key_size" : "3072",
    "issue_date" : 1752048619976
  }, {
    "algorithm" : "SHA256withRSA",
    "certificate" : "certificate text",
    "certificate_id" : "cer-a96ccdb1-5556-4454-a6ed-1415774d6693",
    "expiry_date" : 1769558400000,
    "status" : "INACTIVE",
    "key_size" : "3072",
    "issue_date" : 1753706674547
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 2
  }
}
```


Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.9 Instance Configuration Management

4.9.1 Configuring an Instance

Function

This API is used to configure an IAM Identity Center instance, including identity authentication and session management. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/sso-configuration

Table 4-544 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-545 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-546 Parameters in the request body

Parameter	Mandatory	Type	Description
sso_configuration	Yes	**SSOConfigurationDto** object	Instance configuration.
configuration_type	Yes	String	Configuration type.

Table 4-547 SSOConfigurationDto

Parameter	Mandatory	Type	Description
mfa_mode	No	String	Effective mode of MFA.
no_mfa_signin_behavior	No	String	Available login behavior when an MFA device is not registered.
no_password_signin_behavior	No	String	Login without a password.
allowed_mfa_types	No	Array of strings	Allowed MFA types.
session_configuration	No	**SessionConfigurationDto** object	Session validity configuration.

Table 4-548 SessionConfigurationDto

Parameter	Mandatory	Type	Description
max_authentication_age	Yes	String	Effective time of a session.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-549 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-550 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Configuring an IAM Identity Center service instance, including identity authentication and session management

```
POST https://{hostname}/v1/instances/{instance_id}/sso-configuration

{
  "sso_configuration" : {
    "mfa_mode" : "ALWAYS_ON",
    "no_mfa_signin_behavior" : "ALLOWED",
    "no_password_signin_behavior" : "BLOCKED",
    "allowed_mfa_types" : [ "TOTP" ],
    "session_configuration" : {
      "max_authentication_age" : "PT8H"
    }
  },
  "configuration_type" : "APP_AUTHENTICATION_CONFIGURATION"
}
```

Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.9.2 Querying Instance Configurations

Function

This API is used to query the configurations of an IAM Identity Center instance, including identity authentication and session management. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/sso-configuration

Table 4-551 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-552 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-553 Parameters in the response body

Parameter	Type	Description
sso_configuration	**SSOConfigurationDto** object	IAM Identity Center instance configuration.

Table 4-554 SSOConfigurationDto

Parameter	Type	Description
mfa_mode	String	Effective mode of MFA.
no_mfa_signin_behavior	String	Available login behavior when an MFA device is not registered.
no_password_signin_behavior	String	Login without a password.
allowed_mfa_types	Array of strings	Allowed MFA types.
session_configuration	**SessionConfigurationDto** object	Session validity configuration.

Table 4-555 SessionConfigurationDto

Parameter	Type	Description
max_authentication_age	String	Effective time of a session.

Status code: 400

Table 4-556 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-557 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-558 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Querying configurations of an IAM Identity Center instance, including identity authentication and session management

```
GET https://{hostname}/v1/instances/{instance_id}/sso-configuration
```

Example Response

Status code: 200

Successful.

```
{
  "sso_configuration" : {
    "mfa_mode" : "ALWAYS_ON",
    "no_mfa_signin_behavior" : "ALLOWED",
    "no_password_signin_behavior" : "BLOCKED",
    "allowed_mfa_types" : [ "TOTP" ],
    "session_configuration" : {
      "max_authentication_age" : "PT8H"
    }
  }
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.
404	Forbidden.

Error Codes

For details, see **Error Codes**.

4.10 MFA Configuration Management

4.10.1 Querying MFA Management Configurations

Function

This API is used to query MFA management configurations. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/instances/{instance_id}/mfa-devices/management-settings

Table 4-559 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-560 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-561 Parameters in the response body

Parameter	Type	Description
identity_store_id	String	Globally unique ID of the identity source associated with an IAM Identity Center instance.
user_permission	String	Action allowed for users to perform operations on MFA devices.

Status code: 400

Table 4-562 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-563 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-564 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Querying MFA management configurations

```
GET https://{hostname}/v1/instances/{instance_id}/mfa-devices/management-settings
```

Example Response

Status code: 200

Successful

```
{
  "identity_store_id" : "d-xxxxxx",
  "user_permission" : "READ_ACTIONS"
}
```

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.10.2 Configuring MFA Management

Function

This API is used to configure MFA management. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/instances/{instance_id}/mfa-devices/management-settings

Table 4-565 Path parameters

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Globally unique ID of an IAM Identity Center instance.

Request Parameters

Table 4-566 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-567 Parameters in the request body

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source associated with an IAM Identity Center instance.
user_permission	Yes	String	Action allowed for users to manage MFA.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-568 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-569 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-570 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Configuring MFA management

```
POST https://{hostname}/v1/instances/{instance_id}/mfa-devices/management-settings

{
  "identity_store_id" : "d-xxxxxxx",
  "user_permission" : "READ_ACTIONS"
}
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.11 User Management

4.11.1 Creating a User

Function

This API is used to create an IAM Identity Center user in the specified identity source. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/users

Table 4-571 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**

Request Parameters

Table 4-572 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-573 Parameters in the request body

Parameter	Mandatory	Type	Description
addresses	No	Array of objects	Address list of a user. Array length: **1-1**

Parameter	Mandatory	Type	Description
display_name	Yes	String	Display name of a user. Minimum length: **1** Maximum length: **1024**
emails	Yes	Array of objects	Email address list of a user. Array length: **1-1**
locale	No	String	Geographical area or location of a user. Minimum length: **1** Maximum length: **1024**
name	Yes	Object	User's name.
nickname	No	String	Nickname of a user. Minimum length: **1** Maximum length: **1024**
phone_numbers	No	Array of objects	Phone number list of a user. Array length: **1-1**
preferred_language	No	String	User's preferred language. Minimum length: **1** Maximum length: **1024**
profile_url	No	String	URL associated with a user. Minimum length: **1** Maximum length: **1024**
timezone	No	String	User time zone. Minimum length: **1** Maximum length: **1024**
title	No	String	User title. Minimum length: **1** Maximum length: **1024**
user_name	Yes	String	Username, which uniquely identifies a user. Minimum length: **2** Maximum length: **128**
user_type	No	String	User type. Minimum length: **1** Maximum length: **1024**

Parameter	Mandatory	Type	Description
password_mode	Yes	String	Password initialization mode, which can be one-time password or email address. Enumerated value: • **OTP** • **EMAIL**
enterprise	No	Object	User work information.

Table 4-574 addresses

Parameter	Mandatory	Type	Description
country	No	String	Country or region. Minimum length: **1** Maximum length: **1024**
formatted	No	String	Formatted address to be displayed. Minimum length: **1** Maximum length: **1024**
locality	No	String	Location. Minimum length: **1** Maximum length: **1024**
postal_code	No	String	Postal code. Minimum length: **1** Maximum length: **1024**
primary	No	Boolean	Whether the address is the user's primary address.
region	No	String	Region. Minimum length: **1** Maximum length: **1024**
street_address	No	String	Street. Minimum length: **1** Maximum length: **1024**
type	No	String	Address type. Minimum length: **1** Maximum length: **1024**

Table 4-575 emails

Parameter	Mandatory	Type	Description
primary	Yes	Boolean	Whether the value is the user's primary email address.
type	Yes	String	Email address type. Minimum length: **1** Maximum length: **1024**
value	Yes	String	Email address. Minimum length: **1** Maximum length: **1024**
verification_status	No	String	Verification status of an email address. Enumerated value: • **NOT_VERIFIED** • **VERIFIED**

Table 4-576 name

Parameter	Mandatory	Type	Description
family_name	Yes	String	Family name of a user. Minimum length: **1** Maximum length: **1024**
formatted	No	String	Formatted name to be displayed. Minimum length: **1** Maximum length: **1024**
given_name	Yes	String	Given name of a user. Minimum length: **1** Maximum length: **1024**
honorific_prefix	No	String	Prefix of a user's name. Minimum length: **1** Maximum length: **1024**
honorific_suffix	No	String	Suffix of a user's name. Minimum length: **1** Maximum length: **1024**

Parameter	Mandatory	Type	Description
middle_name	No	String	Middle name of a user. Minimum length: **1** Maximum length: **1024**

Table 4-577 phone_numbers

Parameter	Mandatory	Type	Description
primary	No	Boolean	Whether the value is the user's primary phone number.
type	No	String	Phone number type. Minimum length: **1** Maximum length: **1024**
value	No	String	Phone number. Minimum length: **1** Maximum length: **1024**

Table 4-578 enterprise

Parameter	Mandatory	Type	Description
cost_center	No	String	Cost Center. Minimum length: **1** Maximum length: **1024**
department	No	String	Department. Minimum length: **1** Maximum length: **1024**
division	No	String	Division. Minimum length: **1** Maximum length: **1024**
employee_number	No	String	Employee ID. Minimum length: **1** Maximum length: **1024**
manager	No	Object	Manager.
organization	No	String	Organization. Minimum length: **1** Maximum length: **1024**

Table 4-579 manager

Parameter	Mandatory	Type	Description
value	No	String	Manager. Minimum length: **1** Maximum length: **1024**

Response Parameters

Status code: 201

Table 4-580 Parameters in the response body

Parameter	Type	Description
identity_store_id	String	Globally unique ID of an identity source. Minimum length: **1** Maximum length: **36**
user_id	String	Globally unique ID of an IAM Identity Center user in the identity source. Minimum length: **1** Maximum length: **47**
password	String	One-time password used to initialize the password.

Status code: 400

Table 4-581 Parameters in the response body

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

Status code: 403

Table 4-582 Parameters in the response body

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

Status code: 409

Table 4-583 Parameters in the response body

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

Example Request

Creating an IAM Identity Center user in the specified identity source

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/users

{
  "user_name" : "User name u1",
  "display_name" : "User display name",
  "emails" : [ {
    "primary" : true,
    "type" : "Work",
    "value" : "email@example.com"
  } ],
  "name" : {
    "family_name" : "Family name",
    "given_name" : "Given name"
  },
  "password_mode" : "OTP"
}
```

Example Response

Status code: 201

Successful


```
{
  "identity_store_id" : "d-a00aaaa33f",
  "user_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
  "password" : "one-time-password-123"
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.11.2 Sending an Email Containing a Password Reset Link or Generating a One-Time Password

Function

This API is used to send an email containing a password reset link or generate a one-time password for a user. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/users/{user_id}/reset-password

Table 4-584 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source.

Request Parameters

Table 4-585 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-586 Parameters in the request body

Parameter	Mandatory	Type	Description
mode	Yes	String	Password resetting mode: one-time password or email address.

Response Parameters

Status code: 200

Table 4-587 Parameters in the response body

Parameter	Type	Description
password	String	Password.

Status code: 400

Table 4-588 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-589 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Sending an email containing a password reset link or generating a one-time password for a user

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/users/{user_id}/reset-password

{
  "mode" : "OTP"
}
```

Example Response

Status code: 200

Successful

```
{
  "password" : "pass***"
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.11.3 Listing Users

Function

This API is used to list the IAM Identity Center users in the specified identity source. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/users

Table 4-590 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**

Table 4-591 Query parameters

Parameter	Mandatory	Type	Description
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
user_name	No	String	Username

Request Parameters

Table 4-592 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-593 Parameters in the response body

Parameter	Type	Description
page_info	Object	Pagination information.
users	Array of objects	List of users in the identity source.

Table 4-594 page_info

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**.
current_count	Integer	Number of records returned on this page.

Table 4-595 users

Parameter	Type	Description
addresses	Array of objects	Address list of a user. Array length: **1-1**
display_name	String	Display name of a user. Minimum length: **1** Maximum length: **1024**
emails	Array of objects	Email address list of a user. Array length: **1-1**
external_id	String	Identifier assigned by an external identity source to a resource.
external_ids	Array of objects	External ID list of a user. Array length: **1-10**
identity_store_id	String	Globally unique ID of an identity source. Minimum length: **1** Maximum length: **36**

Parameter	Type	Description
locale	String	Geographical area or location of a user. Minimum length: **1** Maximum length: **1024**
name	Object	User's name.
nickname	String	Nickname of a user. Minimum length: **1** Maximum length: **1024**
phone_numbers	Array of objects	Phone number list of a user. Array length: **1-1**
preferred_language	String	User's preferred language. Minimum length: **1** Maximum length: **1024**
profile_url	String	URL associated with a user. Minimum length: **1** Maximum length: **1024**
timezone	String	User time zone. Minimum length: **1** Maximum length: **1024**
title	String	User title. Minimum length: **1** Maximum length: **1024**
user_id	String	Globally unique ID of an IAM Identity Center user in the identity source. Minimum length: **1** Maximum length: **47**
user_name	String	Username, which uniquely identifies a user. Minimum length: **2** Maximum length: **128**
user_type	String	User type. Minimum length: **1** Maximum length: **1024**
created_at	Long	Timestamp when a user is created.
created_by	String	Creator.
updated_at	Long	Timestamp when a user is updated.
updated_by	String	Updater.

Parameter	Type	Description
enabled	Boolean	Whether a user is enabled.
enterprise	Object	User work information.

Table 4-596 users.addresses

Parameter	Type	Description
country	String	Country or region. Minimum length: **1** Maximum length: **1024**
formatted	String	Formatted address to be displayed. Minimum length: **1** Maximum length: **1024**
locality	String	Location. Minimum length: **1** Maximum length: **1024**
postal_code	String	Postal code. Minimum length: **1** Maximum length: **1024**
primary	Boolean	Whether the address is the user's primary address.
region	String	Region. Minimum length: **1** Maximum length: **1024**
street_address	String	Street. Minimum length: **1** Maximum length: **1024**
type	String	Address type. Minimum length: **1** Maximum length: **1024**

Table 4-597 users.emails

Parameter	Type	Description
primary	Boolean	Whether the value is the user's primary email address.

Parameter	Type	Description
type	String	Email address type. Minimum length: **1** Maximum length: **1024**
value	String	Email address. Minimum length: **1** Maximum length: **1024**
verification_status	String	Verification status of an email address. Enumerated value: • **NOT_VERIFIED** • **VERIFIED**

Table 4-598 users.external_ids

Parameter	Type	Description
id	String	Resource ID issued by an external identity provider. Minimum length: **1** Maximum length: **256**
issuer	String	Issuer of an external ID. Minimum length: **1** Maximum length: **100**

Table 4-599 users.name

Parameter	Type	Description
family_name	String	Family name of a user. Minimum length: **1** Maximum length: **1024**
formatted	String	Formatted name to be displayed. Minimum length: **1** Maximum length: **1024**
given_name	String	Given name of a user. Minimum length: **1** Maximum length: **1024**

Parameter	Type	Description
honorific_prefix	String	Prefix of a user's name. Minimum length: **1** Maximum length: **1024**
honorific_suffix	String	Suffix of a user's name. Minimum length: **1** Maximum length: **1024**
middle_name	String	Middle name of a user. Minimum length: **1** Maximum length: **1024**

Table 4-600 users.phone_numbers

Parameter	Type	Description
primary	Boolean	Whether the value is the user's primary phone number.
type	String	Phone number type. Minimum length: **1** Maximum length: **1024**
value	String	Phone number. Minimum length: **1** Maximum length: **1024**

Table 4-601 enterprise

Parameter	Type	Description
cost_center	String	Cost Center. Minimum length: **1** Maximum length: **1024**
department	String	Department. Minimum length: **1** Maximum length: **1024**
division	String	Division. Minimum length: **1** Maximum length: **1024**

Parameter	Type	Description
employee_number	String	Employee ID. Minimum length: **1** Maximum length: **1024**
manager	Object	Manager.
organization	String	Organization. Minimum length: **1** Maximum length: **1024**

Table 4-602 manager

Parameter	Type	Description
value	String	Manager. Minimum length: **1** Maximum length: **1024**

Status code: 400

Table 4-603 Parameters in the response body

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

Status code: 403

Table 4-604 Parameters in the response body

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 error message.

Example Request

Listing the IAM Identity Center users in the specified identity source

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/users
```

Example Response

Status code: 200

```
{
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  },
  "users" : [ {
    "addresses" : null,
    "display_name" : "Display name of a user",
    "emails" : [ {
      "primary" : true,
      "type" : "Work",
      "value" : "email@example.com"
    } ],
    "external_ids" : null,
    "identity_store_id" : "d-a00aaaa33f",
    "locale" : null,
    "name" : {
      "family_name" : "Family name",
      "formatted" : null,
      "given_name" : "Given name",
      "honorific_prefix" : null,
      "honorific_suffix" : null,
      "middle_name" : null
    },
    "nickname" : null,
    "phone_numbers" : null,
    "preferred_language" : null,
    "profile_url" : null,
    "timezone" : null,
    "title" : null,
    "user_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
    "user_name" : "Username u1",
    "user_type" : null,
    "created_at" : 1687184129925,
    "created_by" : "5146d03d8aaaaaaaaaaabbae60620a5",
    "updated_at" : 1687184129926,
    "updated_by" : "5146d03d8aaaaaaaaaaabbae60620a5",
    "enabled" : true
  } ]
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.11.4 Listing User Login Sessions

Function

This API is used to list login sessions of a specified user. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/users/{user_id}/sessions

Table 4-605 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source.

Request Parameters

Table 4-606 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-607 Parameters in the response body

Parameter	Type	Description
session_list	Array of **UserSessionDto** objects	User login session list.

Table 4-608 UserSessionDto

Parameter	Type	Description
creation_time	Long	Session creation time.
ip_address	String	IP address of a user.
session_id	String	Session ID.
session_not_valid_after	Long	Session expiration time.
user_agent	String	User client information.
user_id	String	Unique user ID.

Status code: 400

Table 4-609 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-610 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying the login session information of a specified user

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/users
```

Example Response

Status code: 200

Successful

```
{
  "session_list" : [ {
    "creation_time" : 1753858567,
    "ip_address" : "your ip",
    "session_id" : "ea70c04b-d510-41c7-b0d1-51d56xxxx",
    "session_not_valid_after" : 1753887367,
    "user_agent" : "[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36]",
    "user_id" : "201dca3f-965b-4311-xxxx-xxxx"
  } ]
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.11.5 Deleting a User

Function

This API is used to delete an IAM Identity Center user based on the user ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/identity-stores/{identity_store_id}/users/{user_id}

Table 4-611 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source Minimum length: **1** Maximum length: **64**

Request Parameters

Table 4-612 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 400

Table 4-613 Parameters in the response body

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

Status code: 403

Table 4-614 Parameters in the response body

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

Status code: 404

Table 4-615 Parameters in the response body

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

Example Request

Deleting an IAM Identity Center user based on the user ID

```
DELETE https://{hostname}/v1/identity-stores/{identity_store_id}/users/{user_id}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.11.6 Enabling a User

Function

This API is used to enable an IAM Identity Center user.

URI

POST /v1/identity-stores/{identity_store_id}/users/{user_id}/enable

Table 4-616 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source.

Request Parameters

Table 4-617 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful.

Status code: 400

Table 4-618 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-619 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 409

Table 4-620 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Enabling an IAM Identity Center user

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/users/{user_id}/enable
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.11.7 Querying User Details

Function

This API is used to query details about an IAM Identity Center user based on the user ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/users/{user_id}

Table 4-621 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source. Minimum length: **1** Maximum length: **64**

Request Parameters

Table 4-622 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-623 Parameters in the response body

Parameter	Type	Description
addresses	Array of objects	Address list of a user. Array length: **1-1**
display_name	String	Display name of a user. Minimum length: **1** Maximum length: **1024**
emails	Array of objects	Email address list of a user. Array length: **1-1**
external_id	String	Identifier assigned by an external identity source to a resource.
external_ids	Array of objects	External ID list of a user. Array length: **1-10**
identity_store_id	String	Globally unique ID of an identity source. Minimum length: **1** Maximum length: **36**
locale	String	Geographical area or location of a user. Minimum length: **1** Maximum length: **1024**
name	Object	User's name.
nickname	String	Nickname of a user. Minimum length: **1** Maximum length: **1024**
phone_numbers	Array of objects	Phone number list of a user. Array length: **1-1**
preferred_language	String	User's preferred language. Minimum length: **1** Maximum length: **1024**
profile_url	String	URL associated with a user. Minimum length: **1** Maximum length: **1024**
timezone	String	User time zone. Minimum length: **1** Maximum length: **1024**

Parameter	Type	Description
title	String	User title. Minimum length: **1** Maximum length: **1024**
user_id	String	Globally unique ID of an IAM Identity Center user in the identity source. Minimum length: **1** Maximum length: **47**
user_name	String	Username, which uniquely identifies a user. Minimum length: **2** Maximum length: **128**
user_type	String	User type. Minimum length: **1** Maximum length: **1024**
created_at	Long	Timestamp when a user is created.
created_by	String	Creator
updated_at	Long	Timestamp when a user is updated.
updated_by	String	Updater.
email_verified	Boolean	Whether the user's primary email address is verified.
enabled	Boolean	Whether a user is enabled.
enterprise	Object	User work information.

Table 4-624 addresses

Parameter	Type	Description
country	String	Country or region. Minimum length: **1** Maximum length: **1024**
formatted	String	Formatted address to be displayed. Minimum length: **1** Maximum length: **1024**
locality	String	Location. Minimum length: **1** Maximum length: **1024**

Parameter	Type	Description
postal_code	String	Postal code. Minimum length: **1** Maximum length: **1024**
primary	Boolean	Whether the address is the user's primary address.
region	String	Region. Minimum length: **1** Maximum length: **1024**
street_address	String	Street. Minimum length: **1** Maximum length: **1024**
type	String	Address type. Minimum length: **1** Maximum length: **1024**

Table 4-625 emails

Parameter	Type	Description
primary	Boolean	Whether the value is the user's primary email address.
type	String	Email address type. Minimum length: **1** Maximum length: **1024**
value	String	Email address. Minimum length: **1** Maximum length: **1024**
verification_status	String	Verification status of an email address. Enumerated value: • **NOT_VERIFIED** • **VERIFIED**

Table 4-626 external_ids

Parameter	Type	Description
id	String	Resource ID issued by an external identity provider. Minimum length: **1** Maximum length: **256**
issuer	String	Issuer of an external ID. Minimum length: **1** Maximum length: **100**

Table 4-627 name

Parameter	Type	Description
family_name	String	Family name of a user. Minimum length: **1** Maximum length: **1024**
formatted	String	Formatted name to be displayed. Minimum length: **1** Maximum length: **1024**
given_name	String	Given name of a user. Minimum length: **1** Maximum length: **1024**
honorific_prefix	String	Prefix of a user's name. Minimum length: **1** Maximum length: **1024**
honorific_suffix	String	Suffix of a user's name. Minimum length: **1** Maximum length: **1024**
middle_name	String	Middle name of a user. Minimum length: **1** Maximum length: **1024**

Table 4-628 phone_numbers

Parameter	Type	Description
primary	Boolean	Whether the value is the user's primary phone number.

Parameter	Type	Description
type	String	Phone number type. Minimum length: **1** Maximum length: **1024**
value	String	Phone number. Minimum length: **1** Maximum length: **1024**

Table 4-629 enterprise

Parameter	Type	Description
cost_center	String	Cost Center. Minimum length: **1** Maximum length: **1024**
department	String	Department. Minimum length: **1** Maximum length: **1024**
division	String	Division. Minimum length: **1** Maximum length: **1024**
employee_number	String	Employee ID. Minimum length: **1** Maximum length: **1024**
manager	Object	Manager.
organization	String	Organization. Minimum length: **1** Maximum length: **1024**

Table 4-630 manager

Parameter	Type	Description
value	String	Manager. Minimum length: **1** Maximum length: **1024**

Status code: 400

Table 4-631 Parameters in the response body

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

Status code: 403

Table 4-632 Parameters in the response body

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

Status code: 404

Table 4-633 Parameters in the response body

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

Example Request

Querying details about an IAM Identity Center user based on the user ID

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/users/{user_id}
```


Example Response

Status code: 200

Successful


```
{
  "addresses" : null,
  "display_name" : "User display name",
  "emails" : [ {
    "primary" : true,
    "type" : "Work",
    "value" : "email@example.com"
  } ],
  "external_ids" : null,
  "identity_store_id" : "d-a00aaaa33f",
  "locale" : null,
  "name" : {
    "family_name" : "Family name",
    "formatted" : null,
    "given_name" : "Given name",
    "honorific_prefix" : null,
    "honorific_suffix" : null,
    "middle_name" : null
  },
  "nickname" : null,
  "phone_numbers" : null,
  "preferred_language" : null,
  "profile_url" : null,
  "timezone" : null,
  "title" : null,
  "user_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
  "user_name" : "User name u1",
  "user_type" : null,
  "created_at" : 1687184129925,
  "created_by" : "5146d03d8aaaaaaaaaaaabbae60620a5",
  "updated_at" : 1687184129926,
  "updated_by" : "5146d03d8aaaaaaaaaaaabbae60620a5",
  "email_verified" : true,
  "enabled" : true
}
```


Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.11.8 Disabling a User

Function

This API is used to disable an IAM Identity Center user. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/users/{user_id}/disable

Table 4-634 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source.

Request Parameters

Table 4-635 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-636 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-637 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 409

Table 4-638 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Disabling an IAM Identity Center user

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/users/{user_id}/disable
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.11.9 Deleting an MFA Device

Function

This API is used to delete an MFA device bound to a user. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/identity-stores/{identity_store_id}/users/{user_id}/mfa-devices/{device_id}

Table 4-639 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source.
device_id	Yes	String	Device ID.

Request Parameters

Table 4-640 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-641 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-642 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-643 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Deleting an MFA device bound to a user

```
DELETE https://{hostname}/v1/identity-stores/{identity_store_id}/users/{user_id}/mfa-devices/{device_id}
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.11.10 Updating a User

Function

This API is used to update the attributes of an IAM Identity Center user based on the user ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/identity-stores/{identity_store_id}/users/{user_id}

Table 4-644 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source. Minimum length: **1** Maximum length: **64**

Request Parameters

Table 4-645 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-646 Parameters in the request body

Parameter	Mandatory	Type	Description
operations	Yes	Array of objects	List of updated user attributes. Array length: **1-100**

Table 4-647 operations

Parameter	Mandatory	Type	Description
attribute_path	Yes	String	Path of the attribute to be updated. Minimum length: **1** Maximum length: **255**
attribute_value	No	String	Attribute value to be updated. If the attribute is an object, set this parameter to the JSON string of the object. If the attribute is **null**, that attribute will be deleted.

Response Parameters

Status code: 400

Table 4-648 Parameters in the response body

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 error message.

Status code: 403

Table 4-649 Parameters in the response body

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

Status code: 404

Table 4-650 Parameters in the response body

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

Example Request

Updating the attributes of an IAM Identity Center user based on the user ID

```
PUT https://{hostname}/v1/identity-stores/{identity_store_id}/users/{user_id}

{
  "operations" : [ {
    "attribute_path" : "emails",
    "attribute_value" : "[{\"primary\":true,\"type\":\"Work\",\"value\":\"new-email@example.com\"}]"
  }, {
    "attribute_path" : "name",
```



```
    "attribute_value": "{\"family_name\":\" Last name\",\"given_name\":\"Given name-new\"}"
  }, {
    "attribute_path" : "display_name",
    "attribute_value": "Display name of the user-new"
  } ]
}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.11.11 Verifying a User's Email Address

Function

This API is used to verify a user's email address. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/users/{user_id}/verify-email

Table 4-651 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source.

Request Parameters

Table 4-652 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-653 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-654 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-655 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 409

Table 4-656 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Verifying a user's email address

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/users/{user_id}/verify-email
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.11.12 Querying a User ID

Function

This API is used to query the user ID in exact match based on either the username or the external identity source ID. They cannot be both specified. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/users/retrieve-user-id

Table 4-657 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**

Request Parameters

Table 4-658 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-659 Parameters in the request body

Parameter	Mandatory	Type	Description
alternate_identifier	Yes	Object	Alternative identifier.

Table 4-660 alternate_identifier

Parameter	Mandatory	Type	Description
external_id	No	Object	Resource ID issued by an external identity provider.
unique_attribute	No	Object	Unique attribute of a specific principal.

Table 4-661 alternate_identifier.external_id

Parameter	Mandatory	Type	Description
id	Yes	String	Resource ID issued by an external identity provider. Minimum length: **1** Maximum length: **256**
issuer	Yes	String	Issuer of an external ID. Minimum length: **1** Maximum length: **100**

Table 4-662 alternate_identifier.unique_attribute

Parameter	Mandatory	Type	Description
attribute_path	Yes	String	Attribute path. Minimum length: **1** Maximum length: **255**
attribute_value	Yes	String	Attribute value. Minimum length: **1** Maximum length: **255**

Response Parameters

Status code: 200

Table 4-663 Parameters in the response body

Parameter	Type	Description
identity_store_id	String	Globally unique ID of an identity source. Minimum length: **1** Maximum length: **36**

Parameter	Type	Description
user_id	String	Globally unique ID of an IAM Identity Center user in the identity source. Minimum length: **1** Maximum length: **47**

Status code: 400

Table 4-664 Parameters in the response body

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

Status code: 403

Table 4-665 Parameters in the response body

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

Example Request

Querying the user ID in exact match based on the username or external identity source ID

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/users/retrieve-user-id

{
  "alternate_identifier" : {
        "unique_attribute" : {
      "attribute_path" : "user_name",
      "attribute_value": "Username u1"
```



```
  }
 }
}
```

Example Response

Status code: 200

Successful

```
{
 "identity_store_id" : "d-a00aaaa33f",
 "user_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9"
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.11.13 Querying Details About Specified Users in Batches

Function

This API is used to query details about specified users in batches. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/users/batch-query

Table 4-666 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Request Parameters

Table 4-667 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-668 Parameters in the request body

Parameter	Mandatory	Type	Description
user_ids	Yes	Array of strings	List of unique user IDs.

Response Parameters

Status code: 200

Table 4-669 Parameters in the response body

Parameter	Type	Description
users	Array of **DescribeUserResp** objects	List of user details.

Table 4-670 DescribeUserResp

Parameter	Type	Description
addresses	Array of **AddressDto** objects	List of user addresses.
display_name	String	Display name of a user.
emails	Array of **EmailDto** objects	Email address list of a user.
external_id	String	Identifier assigned by an external identity source to a resource.

Parameter	Type	Description
external_ids	Array of **ExternalIdDto** objects	External ID list of a user.
identity_store_id	String	Globally unique ID of an identity source.
locale	String	Geographical area or location of a user.
name	**NameDto** object	User's name.
nickname	String	Nickname of a user.
phone_numbers	Array of **PhoneNumberDto** objects	Phone number list of a user.
preferred_language	String	User's preferred language.
profile_url	String	URL associated with a user.
timezone	String	User time zone.
title	String	User title.
user_id	String	Globally unique ID of an IAM Identity Center user in the identity source.
user_name	String	Username, which uniquely identifies a user.
user_type	String	User type.
created_at	Long	Timestamp when a user is created.
created_by	String	Creator.
updated_at	Long	Timestamp when a user is updated.
updated_by	String	Updater.
email_verified	Boolean	Boolean value, indicating whether the email address of a user is verified.
enabled	Boolean	Boolean value, indicating whether a user is enabled.
enterprise	**EnterpriseDto** object	User work information.

Table 4-671 AddressDto

Parameter	Type	Description
country	String	Country or region.
formatted	String	Formatted address to be displayed.
locality	String	Location.
postal_code	String	Postal code.
primary	Boolean	Boolean value, indicating whether this is a user's primary address.
region	String	Region.
street_address	String	Street.
type	String	Address type.

Table 4-672 EmailDto

Parameter	Type	Description
primary	Boolean	Boolean value, indicating whether this is a user's primary email address.
type	String	Email address type.
value	String	Email address.
verification_status	String	Verification status of an email address.

Table 4-673 ExternalIdDto

Parameter	Type	Description
id	String	Resource ID issued by an external identity provider.
issuer	String	Issuer of an external ID.

Table 4-674 NameDto

Parameter	Type	Description
family_name	String	Family name of a user.
formatted	String	Formatted name to be displayed.
given_name	String	Given name of a user.

Parameter	Type	Description
honorific_prefix	String	Prefix of a user's name.
honorific_suffix	String	Suffix of a user's name.
middle_name	String	Middle name of a user.

Table 4-675 PhoneNumberDto

Parameter	Type	Description
primary	Boolean	Boolean value, indicating whether this is a user's primary phone number.
type	String	Phone number type.
value	String	Phone number.

Table 4-676 EnterpriseDto

Parameter	Type	Description
cost_center	String	Cost Center.
department	String	Department.
division	String	Division.
employee_number	String	Employee ID.
manager	**ManagerDto** object	Manager.
organization	String	Organization.

Table 4-677 ManagerDto

Parameter	Type	Description
value	String	Manager information.

Status code: 400

Table 4-678 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-679 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying details about specified users in batches

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/users/batch-query

{
  "user_ids" : [ "c59a3e4f-2cb2-4649-9874-3880664xxx" ]
}
```

Example Response

Status code: 200

Successful

```
{
  "users" : [ {
    "addresses" : [ {
      "country" : "country",
      "formatted" : "formatted",
      "locality" : "locality",
      "postal_code" : "postalCode",
      "primary" : false,
      "region" : "region",
      "street_address" : "streetAddress",
      "type" : "work"
    } ],
    "display_name" : "displayNamexxx",
    "emails" : [ {
      "primary" : true,
      "type" : "work",
      "value" : "xx@xx.com",
```



```
    "verification_status" : "NOT_VERIFIED"
  } ],
  "external_id" : "nickName",
  "external_ids" : [ {
    "id" : "nickName"
  } ],
  "identity_store_id" : "d-a23adaabca",
  "name" : {
    "family_name" : "familyNamedhf",
    "formatted" : "givenNameupdategfgdhf familyNamedhf",
    "given_name" : "givenNameupdategfgdhf"
  },
  "phone_numbers" : [ {
    "primary" : true,
    "type" : "work",
    "value" : "100845277237"
  } ],
  "title" : "title",
  "user_id" : "c59a3e4f-2cb2-4649-9874-38xxxx",
  "user_name" : "your name",
  "created_at" : 1753794283870,
  "created_by" : "SCIM/87905e14-e3ab-43dd-8a48-xxxx",
  "updated_at" : 1753794283878,
  "updated_by" : "SCIM/87905e14-e3ab-43dd-8a48-xxx",
  "email_verified" : false,
  "enabled" : true,
  "enterprise" : {
    "department" : "department",
    "employee_number" : "employeeNumber"
  }
 } ]
}
```


Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.11.14 Registering an MFA device

Function

This API is used to register an MFA device for a user and to return an MFA registration address. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/users/{user_id}/mfa-devices/register-mfa-device

Table 4-680 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source.

Request Parameters

Table 4-681 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-682 Parameters in the response body

Parameter	Type	Description
identity_store_id	String	Globally unique ID of an identity source.
user_id	String	Unique user ID in an identity source.
work_flow	String	One-time random character required for MFA registration.
redirect_url	String	Redirection address after an MFA device is registered.

Status code: 400

Table 4-683 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-684 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Registering an MFA device for a user

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/users/{user_id}/mfa-devices/register-mfa-device
```

Example Response

Status code: 200

Successful

```
{
  "identity_store_id" : "your identity store id",
  "user_id" : "your user id",
  "work_flow" : "random string",
  "redirect_url" : "redirect url"
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.11.15 Listing MFA Devices of a User

Function

This API is used to list MFA devices of a specified user. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/users/retrieve-mfa-devices

Table 4-685 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Request Parameters

Table 4-686 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-687 Parameters in the request body

Parameter	Mandatory	Type	Description
user_list	Yes	Array of **RetrieveMfaDevicesForUserDto** objects	User list.

Table 4-688 RetrieveMfaDevicesForUserDto

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
user_id	Yes	String	Unique user ID.

Response Parameters

Status code: 200

Table 4-689 Parameters in the response body

Parameter	Type	Description
user_mfa_devices_entry_list	Array of **RetrieveMfaDevicesForUserEntryDto** objects	MFA device list of a user.

Table 4-690 RetrieveMfaDevicesForUserEntryDto

Parameter	Type	Description
mfa_devices	Array of **MfaDeviceDto** objects	MFA device list.
user	**RetrieveMfaDevicesForUserDto** object	User information.

Table 4-691 MfaDeviceDto

Parameter	Type	Description
device_id	String	Unique ID of an MFA device.
device_name	String	MFA device name.
display_name	String	Display name of an MFA device.
mfa_type	String	MFA type.
registered_date	Long	Registration time.

Table 4-692 RetrieveMfaDevicesForUserDto

Parameter	Type	Description
identity_store_id	String	Globally unique ID of an identity source.
user_id	String	Unique user ID.

Status code: 400

Table 4-693 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-694 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing MFA devices of a specified user

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/users/retrieve-mfa-devices

{
  "user_list" : [ {
    "identity_store_id" : "d-a23axxxx",
    "user_id" : "201dca3f-965b-4311-8830-dc7953axxxx"
  } ]
}
```

Example Response

Status code: 200

Successful

```
{
  "user_mfa_devices_entry_list" : [ {
    "mfa_devices" : [ {
      "device_id" : "m-fd4e4981d8",
      "device_name" : "MFA1",
      "display_name" : "MFA1",
      "mfa_type" : "TOTP",
      "registered_date" : 1753862382307
    } ],
    "user" : {
      "identity_store_id" : "d-a23adaabca",
      "user_id" : "201dca3f-965b-4311-8830-dc7953aecdcc"
    }
  } ]
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.11.16 Updating the Display Name of an MFA Device

Function

This API is used to update the display name of an MFA device. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/identity-stores/{identity_store_id}/users/{user_id}/mfa-devices/{device_id}

Table 4-695 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source.

Parameter	Mandatory	Type	Description
device_id	Yes	String	MFA device ID.

Request Parameters

Table 4-696 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-697 Parameters in the request body

Parameter	Mandatory	Type	Description
display_name	Yes	String	Display name of an MFA device.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-698 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-699 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Updating the display name of an MFA device

```
PUT https://{hostname}/v1/identity-stores/{identity_store_id}/users/{user_id}/mfa-devices/{device_id}

{
  "display_name" : "my mfa"
}
```

Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.11.17 Deleting User Login Sessions in Batches

Function

This API is used to delete user login sessions in batches. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/users/{user_id}/sessions/batch-delete

Table 4-700 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source.

Request Parameters

Table 4-701 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-702 Parameters in the request body

Parameter	Mandatory	Type	Description
session_ids	Yes	Array of strings	ID of a user login session.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-703 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-704 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Deleting user login sessions in batches

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/users/{user_id}/sessions/batch-delete

{
  "session_ids" : [ "ea70c04b-d510-41c7-b0d1-51d56d1ab7d9" ]
}
```

Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.12 Group Management

4.12.1 Creating a Group

Function

This API is used to create an IAM Identity Center group in the specified identity source. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/groups

Table 4-705 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**

Request Parameters

Table 4-706 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-707 Parameters in the request body

Parameter	Mandatory	Type	Description
description	No	String	Group description. Minimum length: **0** Maximum length: **1024**
display_name	Yes	String	Display name of a group. Minimum length: **1** Maximum length: **1024**

Response Parameters

Status code: 201

Table 4-708 Parameters in the response body

Parameter	Type	Description
group_id	String	Globally unique ID of an IAM Identity Center group in the identity source. Minimum length: **1** Maximum length: **47**
identity_store_id	String	Globally unique ID of an identity source. Minimum length: **1** Maximum length: **36**

Status code: 400

Table 4-709 Parameters in the response body

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

Status code: 403

Table 4-710 Parameters in the response body

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

Status code: 409

Table 4-711 Parameters in the response body

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

Example Request

Creating an IAM Identity Center group in the specified identity source

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/groups

{
  "description" : "Example group",
  "display_name" : "Group name g1"
}
```

Example Response

Status code: 201

Successful

```
{
  "group_id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
  "identity_store_id" : "d-a00aaaa33f"
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.12.2 Listing Groups

Function

This API is used to list the IAM Identity Center groups in the specified identity source. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/groups

Table 4-712 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**

Table 4-713 Query parameters

Parameter	Mandatory	Type	Description
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
display_name	No	String	Fuzzy query of group information by display name.

Request Parameters

Table 4-714 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-715 Parameters in the response body

Parameter	Type	Description
groups	Array of objects	Listed groups.
page_info	Object	Pagination information.

Table 4-716 groups

Parameter	Type	Description
description	String	Group description. Minimum length: **1** Maximum length: **1024**
display_name	String	Display name of a group. Minimum length: **1** Maximum length: **1024**
external_id	String	Identifier assigned by an external identity source to a resource.
external_ids	Array of objects	List of resource IDs issued by an external identity provider. Array length: **0-10**
group_id	String	Globally unique ID of an IAM Identity Center group in the identity source. Minimum length: **1** Maximum length: **47**
identity_store_id	String	Globally unique ID of an identity source. Minimum length: **1** Maximum length: **36**
created_at	Long	Timestamp when a group is created.
created_by	String	Creator.
updated_at	Long	Timestamp when a group is updated.
updated_by	String	Updater

Table 4-717 groups.external_ids

Parameter	Type	Description
id	String	Resource ID issued by an external identity provider. Minimum length: **1** Maximum length: **256**
issuer	String	Issuer of an external ID. Minimum length: **1** Maximum length: **100**

Table 4-718 page_info

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**.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-719 Parameters in the response body

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

Status code: 403

Table 4-720 Parameters in the response body

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

Example Request

Listing the IAM Identity Center groups in the specified identity source

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/groups
```

Example Response

Status code: 200

Successful

```
{
  "groups" : [ {
    "description" : "Example group",
    "display_name" : "Group g1",
    "external_ids" : null,
    "group_id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
    "identity_store_id" : "d-a00aaaa33f",
    "created_at" : 1677175760379,
    "created_by" : "5146d03d8aaaaaaaaaaabbae60620a5",
    "updated_at" : 1677175760379,
    "updated_by" : "5146d03d8aaaaaaaaaaabbae60620a5"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.12.3 Deleting a Group

Function

This API is used to delete an IAM Identity Center group based on the group ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/identity-stores/{identity_store_id}/groups/{group_id}

Table 4-721 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**
group_id	Yes	String	Globally unique ID of an IAM Identity Center group in the identity source. Minimum length: **1** Maximum length: **64**

Request Parameters

Table 4-722 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 400

Table 4-723 Parameters in the response body

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

Status code: 403

Table 4-724 Parameters in the response body

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

Status code: 404

Table 4-725 Parameters in the response body

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

Example Request

Deleting an IAM Identity Center group based on the group ID

```
DELETE https://{hostname}/v1/identity-stores/{identity_store_id}/groups/{group_id}
```


Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.12.4 Updating a Group

Function

This API is used to update the attributes of an IAM Identity Center group based on the group ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/identity-stores/{identity_store_id}/groups/{group_id}

Table 4-726 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**
group_id	Yes	String	Globally unique ID of an IAM Identity Center group in the identity source. Minimum length: **1** Maximum length: **64**

Request Parameters

Table 4-727 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-728 Parameters in the request body

Parameter	Mandatory	Type	Description
operations	Yes	Array of objects	List of updated group attributes. Array length: **1-100**

Table 4-729 operations

Parameter	Mandatory	Type	Description
attribute_path	Yes	String	Attribute to be updated. Minimum length: **1** Maximum length: **255**
attribute_value	No	String	Attribute value to be updated. If the attribute is an object, set this parameter to the JSON string of the object. If the attribute is **null**, that attribute will be deleted.

Response Parameters

None

Example Request

Updating the attributes of an IAM Identity Center group based on the group ID

```
PUT https://{hostname}/v1/identity-stores/{identity_store_id}/groups/{group_id}

{
  "operations" : [ {
    "attribute_path" : "description",
```



```
"attribute_value": "Description of updating a group"
  } ]
}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.12.5 Querying Group Details

Function

This API is used to query details about an IAM Identity Center group based on the group ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/groups/{group_id}

Table 4-730 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**
group_id	Yes	String	Globally unique ID of an IAM Identity Center group in the identity source. Minimum length: **1** Maximum length: **64**

Request Parameters

Table 4-731 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-732 Parameters in the response body

Parameter	Type	Description
description	String	Group description. Minimum length: **1** Maximum length: **1024**
display_name	String	Display name of a group. Minimum length: **1** Maximum length: **1024**
external_id	String	Identifier assigned by an external identity source to a resource.
external_ids	Array of objects	List of resource IDs issued by an external identity provider. Array length: **1-10**
group_id	String	Globally unique ID of an IAM Identity Center group in the identity source. Minimum length: **1** Maximum length: **47**
identity_store_id	String	Globally unique ID of an identity source. Minimum length: **1** Maximum length: **36**
created_at	Long	Timestamp when a group is created.
created_by	String	Creator.
updated_at	Long	Timestamp when a group is updated.

Parameter	Type	Description
updated_by	String	Updater.

Table 4-733 external_ids

Parameter	Type	Description
id	String	Resource ID issued by an external identity provider. Minimum length: **1** Maximum length: **256**
issuer	String	Issuer of an external ID. Minimum length: **1** Maximum length: **100**

Example Request

Querying details about an IAM Identity Center group based on the group ID

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/groups/{group_id}
```

Example Response

Status code: 200

```
{
  "description" : "Example group",
  "display_name" : "Group name g1",
  "external_ids" : null,
  "group_id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
  "identity_store_id" : "d-a00aaaa33f",
  "created_at" : 1677175760379,
  "created_by" : "5146d03d8aaaaaaaaaaaabbae60620a5",
  "updated_at" : 1677175760379,
  "updated_by" : "5146d03d8aaaaaaaaaaaabbae60620a5"
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.12.6 Querying a Group ID

Function

This API is used to query the group ID in exact match based on either the display name or the external identity source ID. They cannot be both specified. It can be

called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/groups/retrieve-group-id

Table 4-734 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**

Request Parameters

Table 4-735 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-736 Parameters in the request body

Parameter	Mandatory	Type	Description
alternate_identifier	Yes	Object	Alternative identifier.

Table 4-737 alternate_identifier

Parameter	Mandatory	Type	Description
external_id	No	Object	Resource ID issued by an external identity provider.
unique_attribute	No	Object	Unique attribute of a specific principal.

Table 4-738 alternate_identifier.external_id

Parameter	Mandatory	Type	Description
id	Yes	String	Resource ID issued by an external identity provider. Minimum length: **1** Maximum length: **256**
issuer	Yes	String	Issuer of an external ID. Minimum length: **1** Maximum length: **100**

Table 4-739 alternate_identifier.unique_attribute

Parameter	Mandatory	Type	Description
attribute_path	Yes	String	Attribute path. Minimum length: **1** Maximum length: **255**
attribute_value	Yes	String	Attribute value. Minimum length: **1** Maximum length: **255**

Response Parameters

Status code: 200

Table 4-740 Parameters in the response body

Parameter	Type	Description
group_id	String	Globally unique ID of an IAM Identity Center group in the identity source. Minimum length: **1** Maximum length: **47**
identity_store_id	String	Globally unique ID of an identity source. Minimum length: **1** Maximum length: **36**

Status code: 400

Table 4-741 Parameters in the response body

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

Status code: 403

Table 4-742 Parameters in the response body

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

Example Request

Querying the group ID in exact match based on either the display name or the external identity source ID

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/groups/retrieve-group-id

{
  "alternate_identifier" : {
        "unique_attribute" : {
      "attribute_path" : "display_name",
      "attribute_value": "Group name g1"
    }
  }
}
```

Example Response

Status code: 200

Successful

```
{
  "group_id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
  "identity_store_id" : "d-a00aaaa33f"
}
```


Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.12.7 Querying Details About Specified User Groups in Batches

Function

This API is used to query details about specified user groups in batches. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/groups/batch-query

Table 4-743 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Request Parameters

Table 4-744 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-745 Parameters in the request body

Parameter	Mandatory	Type	Description
group_ids	Yes	Array of strings	List of unique user group IDs.

Response Parameters

Status code: 200

Table 4-746 Parameters in the response body

Parameter	Type	Description
groups	Array of **DescribeGroupResp** objects	User group list.

Table 4-747 DescribeGroupResp

Parameter	Type	Description
description	String	Group description.
display_name	String	Display name of a group.
external_id	String	Identifier assigned by an external identity source to a resource.
external_ids	Array of **ExternalIdDto** objects	List of resource IDs issued by an external identity provider.
group_id	String	Globally unique ID of an IAM Identity Center group in the identity source.
identity_store_id	String	Globally unique ID of an identity source.
created_at	Long	Creation timestamp.
created_by	String	Creator.
updated_at	Long	Update timestamp.
updated_by	String	Updater.

Table 4-748 ExternalIdDto

Parameter	Type	Description
id	String	Resource ID issued by an external identity provider.
issuer	String	Issuer of an external ID.

Status code: 400

Table 4-749 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-750 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying details about specified user groups in batches

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/groups/batch-query

{
  "group_ids" : [ "749aa4a2-6774-4fbb-aefa-94c68cf15a81" ]
}
```

Example Response

Status code: 200

Successful

```
[ {
  "description" : "description",
  "display_name" : "group test",
  "group_id" : "749aa4a2-6774-4fbb-aefa-94c68cxxxx1",
  "identity_store_id" : "d-a23adaxxxx",
  "created_at" : 1753794050369,
  "created_by" : "9ec6f4f5dd28485cbcdd9804c5428331",
  "updated_at" : 1753794050369,
  "updated_by" : "9ec6f4f5dd28485cbcdd9804c5428331"
} ]
```


Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.13 Group Membership Management

4.13.1 Adding a User to a Group

Function

This API is used to add a user to a group in the same identity source. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/group-memberships

Table 4-751 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**

Request Parameters

Table 4-752 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-753 Parameters in the request body

Parameter	Mandatory	Type	Description
group_id	Yes	String	Globally unique ID of an IAM Identity Center group in the identity source. Minimum length: **1** Maximum length: **47**
member_id	Yes	Object	Group member ID.

Table 4-754 member_id

Parameter	Mandatory	Type	Description
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source. Minimum length: **1** Maximum length: **47**

Response Parameters

Status code: 200

Table 4-755 Parameters in the response body

Parameter	Type	Description
identity_store_id	String	Globally unique ID of an identity source. Minimum length: **1** Maximum length: **36**

Parameter	Type	Description
membership_id	String	Globally unique ID of a group membership in the identity source. Minimum length: **1** Maximum length: **47**

Status code: 400

Table 4-756 Parameters in the response body

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

Status code: 403

Table 4-757 Parameters in the response body

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

Example Request

Adding a user to a group in the same identity source

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/group-memberships

{
  "group_id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
  "member_id" : {
    "user_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9"
  }
}
```


Example Response

Status code: 200

Successful

```
{
  "identity_store_id" : "d-a00aaaa33f",
  "membership_id" : "2b0aa970-7aa4-3aaf-0aae-7a2eaaaae3a5"
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.13.2 Listing Users in a Group

Function

This API is used to list users in a group based on the group ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/group-memberships

Table 4-758 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**

Table 4-759 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**

Parameter	Mandatory	Type	Description
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**
group_id	Yes	String	Globally unique ID of an IAM Identity Center group in the identity source. Minimum length: **1** Maximum length: **64**

Request Parameters

Table 4-760 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-761 Parameters in the response body

Parameter	Type	Description
group_memberships	Array of objects	Matched group members for a query.
page_info	Object	Pagination information.

Table 4-762 group_memberships

Parameter	Type	Description
group_id	String	Globally unique ID of an IAM Identity Center group in the identity source. Minimum length: **1** Maximum length: **47**
identity_store_id	String	Globally unique ID of an identity source. Minimum length: **1** Maximum length: **36**
member_id	Object	Group member ID.
membership_id	String	Globally unique ID of a group membership in the identity source. Minimum length: **1** Maximum length: **47**

Table 4-763 group_memberships.member_id

Parameter	Type	Description
user_id	String	Globally unique ID of an IAM Identity Center user in the identity source. Minimum length: **1** Maximum length: **47**

Table 4-764 page_info

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**.
current_count	Integer	Number of records returned on this page.

Example Request

Listing users in a group based on the group ID

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/group-memberships
```


Example Response

Status code: 200


```
{
  "group_memberships" : [ {
    "group_id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
    "identity_store_id" : "d-a00aaaa33f",
    "member_id" : {
      "user_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9"
    },
    "membership_id" : "2b0aa970-7aa4-3aaf-0aae-7a2eaaaae3a5"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```


Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.13.3 Listing Groups to which a User is Added

Function

This API is used to list the groups to which a user is added based on the user ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/group-memberships-for-member

Table 4-765 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**

Table 4-766 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results returned for each request. Minimum value: **1** Maximum value: **100** Default value: **100**
marker	No	String	Pagination marker. Minimum length: **24** Maximum length: **24**
user_id	Yes	String	Unique ID of a user. Minimum length: **1** Maximum length: **64**

Request Parameters

Table 4-767 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-768 Parameters in the response body

Parameter	Type	Description
group_memberships	Array of objects	Matched group members for a query.
page_info	Object	Pagination information.

Table 4-769 group_memberships

Parameter	Type	Description
group_id	String	Globally unique ID of an IAM Identity Center group in the identity source.
identity_store_id	String	Globally unique ID of an identity source.
member_id	Object	Group member ID.
membership_id	String	Globally unique ID of a group membership in the identity source.

Table 4-770 group_memberships.member_id

Parameter	Type	Description
user_id	String	Globally unique ID of an IAM Identity Center user in the identity source. Minimum length: **1** Maximum length: **47**

Table 4-771 page_info

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**.
current_count	Integer	Number of records returned on this page.

Status code: 400

Table 4-772 Parameters in the response body

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 error message.

Status code: 403

Table 4-773 Parameters in the response body

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

Example Request

Listing the groups to which a user is added based on the user ID

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/group-memberships-for-member
```

Example Response

Status code: 200

Successful

```
{
  "group_memberships" : [ {
    "group_id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
    "identity_store_id" : "d-a00aaaa33f",
    "member_id" : {
      "user_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9"
    },
    "membership_id" : "2b0aa970-7aa4-3aaf-0aae-7a2eaaaae3a5"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.13.4 Removing a User from a Group

Function

This API is used to remove a user from a group based on the group membership ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/identity-stores/{identity_store_id}/group-memberships/{membership_id}

Table 4-774 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**
membership_id	Yes	String	Globally unique ID of a group membership in the identity source. Minimum length: **1** Maximum length: **64**

Request Parameters

Table 4-775 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 400

Table 4-776 Parameters in the response body

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

Status code: 403

Table 4-777 Parameters in the response body

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

Example Request

Removing a user from a group based on the group membership ID

```
DELETE https://{hostname}/v1/identity-stores/{identity_store_id}/group-memberships/{membership_id}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.13.5 Querying the Group Membership

Function

This API is used to query details about the group membership based on the group membership ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/group-memberships/{membership_id}

Table 4-778 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**
membership_id	Yes	String	Globally unique ID of a group membership in the identity source. Minimum length: **1** Maximum length: **64**

Request Parameters

Table 4-779 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Response Parameters

Status code: 200

Table 4-780 Parameters in the response body

Parameter	Type	Description
group_id	String	Globally unique ID of an IAM Identity Center group in the identity source. Minimum length: **1** Maximum length: **47**
identity_store_id	String	Globally unique ID of an identity source. Minimum length: **1** Maximum length: **36**
member_id	Object	Group member ID.
membership_id	String	Globally unique ID of a group membership in the identity source. Minimum length: **1** Maximum length: **47**

Table 4-781 member_id

Parameter	Type	Description
user_id	String	Globally unique ID of an IAM Identity Center user in the identity source. Minimum length: **1** Maximum length: **47**

Status code: 400

Table 4-782 Parameters in the response body

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

Status code: 403

Table 4-783 Parameters in the response body

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

Example Request

Querying details about the group membership based on the group membership ID

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/group-memberships/{membership_id}
```

Example Response

Status code: 200

Successful

```
{
  "group_id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
  "identity_store_id" : "d-a00aaaa33f",
  "member_id" : {
    "user_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9"
  },
  "membership_id" : "2b0aa970-7aa4-3aaf-0aae-7a2eaaaae3a5"
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.13.6 Querying the Group Membership ID

Function

This API is used to query the group membership ID based on the user ID and group ID. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/group-memberships/retrieve-group-membership-id

Table 4-784 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**

Request Parameters

Table 4-785 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-786 Parameters in the request body

Parameter	Mandatory	Type	Description
group_id	Yes	String	Globally unique ID of an IAM Identity Center group in the identity source. Minimum length: **1** Maximum length: **47**
member_id	Yes	Object	Group member ID.

Table 4-787 member_id

Parameter	Mandatory	Type	Description
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source. Minimum length: **1** Maximum length: **47**

Response Parameters

Status code: 200

Table 4-788 Parameters in the response body

Parameter	Type	Description
identity_store_id	String	Globally unique ID of an identity source.
membership_id	String	Globally unique ID of a group membership in the identity source.

Status code: 400

Table 4-789 Parameters in the response body

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

Status code: 403

Table 4-790 Parameters in the response body

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

Example Request

Querying the group membership ID based on the user ID and group ID

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/group-memberships/retrieve-group-membership-id
```



```
{
  "group_id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
  "member_id" : {
    "user_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9"
  }
}
```

Example Response

Status code: 200

Successful

```
{
  "identity_store_id" : "d-a00aaaa33f",
  "membership_id" : "2b0aa970-7aa4-3aaf-0aae-7a2eaaaae3a5"
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.13.7 Querying Whether a User Is a Member of a Group

Function

This API is used to query whether a user is a member of a group based on the user ID and group ID list. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/is-member-in-groups

Table 4-791 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source. Minimum length: **12** Maximum length: **12**

Request Parameters

Table 4-792 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required. Maximum length: **2048**

Table 4-793 Parameters in the request body

Parameter	Mandatory	Type	Description
group_ids	Yes	Array of strings	Group ID list. Minimum length: **1** Maximum length: **47** Array length: **1-100**
member_id	Yes	Object	Group member ID.

Table 4-794 member_id

Parameter	Mandatory	Type	Description
user_id	Yes	String	Globally unique ID of an IAM Identity Center user in the identity source. Minimum length: **1** Maximum length: **47**

Response Parameters

Status code: 200

Table 4-795 Parameters in the response body

Parameter	Type	Description
results	Array of objects	Result list, which indicates whether a user is in a group. Array length: **1-100**

Table 4-796 results

Parameter	Type	Description
group_id	String	Globally unique ID of an IAM Identity Center group in the identity source. Minimum length: **1** Maximum length: **47**
member_id	Object	Group member ID.
membership_exists	Boolean	Whether a user is in a group.

Table 4-797 results.member_id

Parameter	Type	Description
user_id	String	Globally unique ID of an IAM Identity Center user in the identity source. Minimum length: **1** Maximum length: **47**

Status code: 400

Table 4-798 Parameters in the response body

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

Status code: 403

Table 4-799 Parameters in the response body

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 error message.

Status code: 404

Table 4-800 Parameters in the response body

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

Example Request

Querying whether a user is a member of a group based on the user ID and group ID list

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/is-member-in-groups

{
  "group_ids" : [ "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a" ],
  "member_id" : {
    "user_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9"
  }
}
```

Example Response

Status code: 200

Successful

```
{
  "results" : [ {
    "group_id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
    "member_id" : {
      "user_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9"
    },
    "membership_exists" : true
  } ]
}
```


Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.14 Identity Provider Management

4.14.1 Creating External Identity Provider Configurations

Function

This API is used to create configurations for an external identity provider. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/external-idp

Table 4-801 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Request Parameters

Table 4-802 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-803 Parameters in the request body

Parameter	Mandatory	Type	Description
idp_saml_metadata	No	String	SAML metadata of an identity provider. Either the SAML settings or the SAML metadata of an identity provider must be configured.
idp_certificate	No	String	Identity provider certificate, which is used together with the identity provider's SAML settings.
idp_saml_config	No	**idp_saml_config** object	SAML settings of an identity provider. Either the SAML settings or the SAML metadata of an identity provider must be configured.

Table 4-804 idp_saml_config

Parameter	Mandatory	Type	Description
entity_id	No	String	Issuer ID of an identity provider.
login_url	No	String	Login link of an identity provider.

Response Parameters

Status code: 201

Table 4-805 Parameters in the response body

Parameter	Type	Description
hws_sp_saml_config	**SPSAMLConfig** object	Service provider configuration.
idp_certificate_id	String	Globally unique ID of an identity provider certificate.
idp_certificate_ids	Array of strings	List of globally unique IDs of identity provider certificates.
idp_id	String	Globally unique ID of an external identity provider.

Table 4-806 SPSAMLConfig

Parameter	Type	Description
acs_url	String	Response address of a service provider's assertion.
issuer	String	Service provider issuer.
metadata	String	Service provider metadata.

Status code: 400

Table 4-807 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-808 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Creating configurations for an external identity provider

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/external-idp

{
  "idp_saml_metadata" : "<?xml version=\"1.0\" encoding=\"utf-8\"?><EntityDescriptor ID=
\"_678cd4a8-4915-4e2d-a4ce-6**********cd/saml2\" /></IDPSSODescriptor></EntityDescriptor>"
}
```

Example Response

Status code: 201

Successful

```
{
  "hws_sp_saml_config" : {
    "acs_url" : "https://cn-north-4-signin.huaweicloud.com/v1/platform/saml/acs/xxxxxxx",
    "issuer" : "https://cn-north-4.signin.huaweicloud.com/platform/saml/xxxxxx",
    "metadata" : "<?xml version=\"1.0\" encoding=\"UTF-8\"?>xxxxxxx</md:EntityDescriptor>"
  },
  "idp_certificate_id" : "553523a6-ebde-4570-xxxxxxx",
  "idp_certificate_ids" : [ "553523a6-ebde-4570-xxxxxxx" ],
  "idp_id" : "a48e3f1b-59f8-4b8f-xxxxxxx"
}
```

Status Codes

Status Code	Description
201	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.14.2 Querying External Identity Provider Configurations

Function

This API is used to query configurations for an external identity provider. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/external-idp

Table 4-809 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Request Parameters

Table 4-810 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-811 Parameters in the response body

Parameter	Type	Description
associations	Array of **ExternalIdpConfigurationDto** objects	External identity provider configuration.

Table 4-812 ExternalIdpConfigurationDto

Parameter	Type	Description
idp_certificate_ids	Array of **IdpCertificateBody** objects	Globally unique ID of an identity provider certificate.
idp_id	String	Globally unique ID of an identity provider.
idp_saml_config	**IdpSAMLConfig** object	Identity provider configuration.
is_enabled	Boolean	Whether an identity provider is enabled.

Table 4-813 IdpCertificateBody

Parameter	Type	Description
certificate_id	String	Globally unique ID of a certificate.
status	String	Certificate status.

Table 4-814 IdpSAMLConfig

Parameter	Type	Description
entity_id	String	Issuer ID of an identity provider.
login_url	String	Login link of an identity provider.
want_request_signed	Boolean	Whether SAML request signature verification is required.

Status code: 400

Table 4-815 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-816 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying configurations for an external identity provider

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/external-idp
```

Example Response

Status code: 200

Successful

```
{
  "associations" : [ {
```



```
    "idp_certificate_ids" : [ {
      "certificate_id" : "553523a6-ebde-4570-9409-xxxxxx",
      "status" : "ACTIVE"
    } ],
    "idp_id" : "a48e3f1b-59f8-4b8f-9944-795xxx",
    "idp_saml_config" : {
      "entity_id" : "https://sts.windows.net/36118e7b-55b4-4a70-8d9f-xxxxx/",
      "login_url" : "https://login.microsoftonline.com/36118e7b-55b4-4a70-xxxxxx/saml2",
      "want_request_signed" : false
    },
    "is_enabled" : true
  } ]
}
```


Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.14.3 Enabling an External Identity Provider

Function

This API is used to enable an external identity provider. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/enable

Table 4-817 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
idp_id	Yes	String	Globally unique ID of an external identity provider.

Request Parameters

Table 4-818 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-819 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-820 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Enabling an external identity provider

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/enable
```


Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.14.4 Disabling an External Identity Provider

Function

This API is used to disable an external identity provider. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/disable

Table 4-821 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
idp_id	Yes	String	Globally unique ID of an external identity provider.

Request Parameters

Table 4-822 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-823 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-824 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Disabling an external identity provider

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/disable
```


Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.14.5 Deleting Configurations of an External Identity Provider

Function

This API is used to delete configurations of an external identity provider. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}

Table 4-825 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
idp_id	Yes	String	Globally unique ID of an external identity provider.

Request Parameters

Table 4-826 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-827 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-828 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Deleting configurations of an external identity provider

```
DELETE https://{hostname}/v1/identity-stores/{identity_store_id}/external-idp/{idp_id}
```


Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.14.6 Updating Configurations of an External Identity Provider

Function

This API is used to update configurations of an external identity provider. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}

Table 4-829 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
idp_id	Yes	String	Globally unique ID of an external identity provider.

Request Parameters

Table 4-830 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-831 Parameters in the request body

Parameter	Mandatory	Type	Description
entity_id	Yes	String	Issuer ID of an identity provider.
login_url	Yes	String	Login link of an identity provider.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-832 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-833 Parameters in the response body

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

Parameter	Type	Description
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Updating configurations of an external identity provider

```
PUT https://{hostname}/v1/identity-stores/{identity_store_id}/external-idp/{idp_id}

{
  "entity_id" : "https://sts.windows.net/36118e7b-55b4-4a70-xxxxx/",
  "login_url" : "https://login.microsoftonline.com/36118e7b-55b4-xxxxx/saml2"
}
```

Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.14.7 Listing External Identity Provider Certificates

Function

This API is used to list external identity provider certificates. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/certificate

Table 4-834 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
idp_id	Yes	String	Globally unique ID of an external identity provider.

Request Parameters

Table 4-835 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-836 Parameters in the response body

Parameter	Type	Description
idp_certificates	Array of **IdpCertificate** objects	List of external identity provider certificates.

Table 4-837 IdpCertificate

Parameter	Type	Description
certificate_id	String	Globally unique ID of a certificate.
issuer_name	String	Issuer of an identity provider.
not_after	Number	Certificate validity period.
not_before	Number	Certificate validity period.
public_key	String	Certificate public key.
serial_number	Number	Certificate SN.

Parameter	Type	Description
serial_number_string	String	Certificate SN text.
signature_algorithm_name	String	Signature algorithm.
subject_name	String	Subject.
version	Number	Version.
x509_Certificate_in_pem	String	X.509 certificate.

Status code: 400

Table 4-838 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-839 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing external identity provider certificates

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/certificate
```

Example Response

Status code: 200

Successful

```
{
  "idp_certificates" : [ {
    "certificate_id" : "47e2272e-7dc9-4dd0-880b-9exxxxxx",
    "issuer_name" : "CN=Microsoft Azure Federated SSO Certificate",
    "not_after" : 1799587006000,
    "not_before" : 1704892606000,
    "public_key" : "your public key",
    "serial_number" : 1.0778418080746175E38,
    "serial_number_string" : "107784180807461748442456173960326386288",
    "signature_algorithm_name" : "SHA256withRSA",
    "subject_name" : "CN=Microsoft Azure Federated SSO Certificate",
    "version" : 3,
    "x509_Certificate_in_pem" : "X509 Certificate"
  } ]
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.14.8 Importing External Identity Provider Certificates

Function

This API is used to import external identity provider certificates. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/certificate

Table 4-840 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
idp_id	Yes	String	Globally unique ID of an external identity provider.

Request Parameters

Table 4-841 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-842 Parameters in the request body

Parameter	Mandatory	Type	Description
x509_certificate_in_pem	Yes	String	Identity provider certificate content in the PEM format.
certificate_use	Yes	String	Usage of an identity provider certificate. Currently, only signature is supported.

Response Parameters

Status code: 200

Table 4-843 Parameters in the response body

Parameter	Type	Description
certificate_id	String	Globally unique ID of a certificate.

Status code: 400

Table 4-844 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-845 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Importing external identity provider certificates

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/certificate

{
  "x509_certificate_in_pem" : "-----BEGIN CERTIFICATE-----*************-----END CERTIFICATE-----\r\n",
  "certificate_use" : "SIGNING"
}
```

Example Response

Status code: 200

Successful

```
{
  "certificate_id" : "cef00a42-28a6-4218-a137-xxxxxxxx"
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.14.9 Deleting External Identity Provider Certificates

Function

This API is used to delete external identity provider certificates. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/certificate/{certificate_id}

Table 4-846 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
certificate_id	Yes	String	Globally unique ID of a certificate in the identity source.
idp_id	Yes	String	Globally unique ID of an external identity provider.

Request Parameters

Table 4-847 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-848 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-849 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Deleting external identity provider certificates

```
DELETE https://{hostname}/v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/certificate/{certificate_id}
```

Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.15 Automatic Provisioning Management

4.15.1 Enabling Automatic Provisioning

Function

This API is used to enable automatic provisioning and automatic SCIM synchronization. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/provision-tenant

Table 4-850 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Request Parameters

Table 4-851 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 201

Table 4-852 Parameters in the response body

Parameter	Type	Description
creation_time	Number	Creation time.
scim_endpoint	String	SCIM endpoint.

Parameter	Type	Description
tenant_id	String	Globally unique ID generated after auto-provisioning is enabled.

Status code: 400

Table 4-853 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-854 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Enabling automatic provisioning and automatic SCIM synchronization

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/provision-tenant
```

Example Response

Status code: 201

Successful

```
{
  "creation_time" : 1754277890722,
  "scim_endpoint" : "https://scim.cn-north-4.myhuaweicloud.com/e0d69be4-ee68-4653-97e4-9e8xxxxx/
scim/v2/",
  "tenant_id" : "e0d69be4-ee68-4653-97e4-9exxxx"
}
```


Status Codes

Status Code	Description
201	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.15.2 Checking Automatic Provisioning

Function

This API is used to check whether SCIM automatic provisioning is enabled. It returns detailed provisioning information if the function is enabled. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/provision-tenant

Table 4-855 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Request Parameters

Table 4-856 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-857 Parameters in the response body

Parameter	Type	Description
provisioning_tenants	Array of **ProvisioningTenant** objects	SCIM automatic provisioning information.

Table 4-858 ProvisioningTenant

Parameter	Type	Description
creation_time	Number	Creation time.
scim_endpoint	String	SCIM endpoint.
tenant_id	String	Globally unique ID generated after auto-provisioning is enabled.

Status code: 400

Table 4-859 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-860 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Checking whether SCIM automatic provisioning is enabled. It returns detailed provisioning information if the function is enabled.

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/provision-tenant
```

Example Response

Status code: 200

Successful

```
{
  "provisioning_tenants" : [ {
    "creation_time" : 1754277890722,
    "scim_endpoint" : "https://scim.cn-north-4.myhuaweicloud.com/e0d69be4-ee68-4653-97xxxxxx/
scim/v2/",
    "tenant_id" : "e0d69be4-ee68-4653-97e4-9exxxxxx"
  } ]
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.15.3 Deleting Automatic Provisioning

Function

This API is used to delete automatic provisioning. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/identity-stores/{identity_store_id}/tenant/{tenant_id}

Table 4-861 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
tenant_id	Yes	String	Globally unique ID of an automatic provisioning.

Request Parameters

Table 4-862 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-863 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-864 Parameters in the response body

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

Parameter	Type	Description
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-865 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Deleting automatic provisioning

```
DELETE https://{hostname}/v1/identity-stores/{identity_store_id}/tenant/{tenant_id}
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.15.4 Creating an Access Token

Function

This API is used to create an access token. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/tenant/{tenant_id}/bearer-token

Table 4-866 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
tenant_id	Yes	String	Globally unique ID of an automatic provisioning.

Request Parameters

Table 4-867 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 201

Table 4-868 Parameters in the response body

Parameter	Type	Description
creation_time	Number	Creation time.
expiration_time	Number	Expiration time.
token	String	Access token.
token_id	String	Globally unique ID of an access token.

Status code: 400

Table 4-869 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-870 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Creating an access token

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/tenant/{tenant_id}/bearer-token
```

Example Response

Status code: 201

Successful

```
{
  "creation_time" : 1754278569275,
  "expiration_time" : 1785814569000,
  "token" : "eyJraWQiOiJmZUV4U0oxRV**********83yzVQVY",
  "token_id" : "715ad873-3b32-48a3-a08f-50xxxxx"
}
```

Status Codes

Status Code	Description
201	Successful.
400	Bad request.

Status Code	Description
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.15.5 Listing Access Tokens

Function

This API is used to list access tokens. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/tenant/{tenant_id}/bearer-token

Table 4-871 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
tenant_id	Yes	String	Globally unique ID of an automatic provisioning.

Request Parameters

Table 4-872 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-873 Parameters in the response body

Parameter	Type	Description
bearer_tokens	Array of **BearerToken** objects	Access token list.

Table 4-874 BearerToken

Parameter	Type	Description
creation_time	Number	Creation time.
expiration_time	Number	Expiration time.
token_id	String	Globally unique ID of an access token.

Status code: 400

Table 4-875 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-876 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Listing access tokens


```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/tenant/{tenant_id}/bearer-token
```

Example Response

Status code: 200

Successful

```
{
  "bearer_tokens" : [ {
    "creation_time" : 1754277891140,
    "expiration_time" : 1785813891000,
    "token_id" : "5bd76fe3-48cc-4e4b-a235-a4e6xxxx"
  }, {
    "creation_time" : 1754278569276,
    "expiration_time" : 1785814569000,
    "token_id" : "715ad873-3b32-48a3-a08f-50fxxxxxx7"
  } ]
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.15.6 Deleting an Access Token

Function

This API is used to delete an access token. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/identity-stores/{identity_store_id}/tenant/{tenant_id}/bearer-token/{token_id}

Table 4-877 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of an automatic provisioning.
token_id	Yes	String	Globally unique ID of an access token.

Request Parameters

Table 4-878 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-879 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-880 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Parameter	Type	Description
encoded_authorization_message	String	Encrypted error message.

Status code: 404

Table 4-881 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Example Request

Deleting an access token

```
DELETE https://{hostname}/v1/identity-stores/{identity_store_id}/tenant/{tenant_id}/bearer-token/{token_id}
```

Example Response

None

Status Codes

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

Error Codes

For details, see **Error Codes**.

4.16 Identity Source Quota Management

4.16.1 Querying Identity Source Quotas

Function

This API is used to query identity source quotas. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/identity-store-summary

Table 4-882 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Request Parameters

Table 4-883 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-884 Parameters in the response body

Parameter	Type	Description
users	Long	Number of created users.
users_quota	Long	User quota.
groups	Long	Number of created user groups.
groups_quota	Long	User group quota.

Status code: 400

Table 4-885 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-886 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying identity source quotas

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/identity-store-summary
```

Example Response

Status code: 200

Successful

```
{
  "users" : 1,
  "users_quota" : 50000,
  "groups" : 0,
  "groups_quota" : 10000
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.17 Custom Password Policy Management

4.17.1 Querying Custom Password Policies

Function

This API is used to query custom password policies. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/password-policy

Table 4-887 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Request Parameters

Table 4-888 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-889 Parameters in the response body

Parameter	Type	Description
password_policy	**PasswordPolicyDto** object	Custom password policy information.

Table 4-890 PasswordPolicyDto

Parameter	Type	Description
minimum_password_length	Integer	Minimum password length.
require_lowercase_characters	Boolean	Whether lowercase letters are required.
require_numbers	Boolean	Whether digits are required.
require_symbols	Boolean	Whether special characters are required.
require_uppercase_characters	Boolean	Whether uppercase letters are required.
max_password_age	Integer	Password validity period.
password_reuse_prevention	Integer	Password reuse limit. The default value is 1.

Status code: 400

Table 4-891 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-892 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying custom password policies

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/password-policy
```

Example Response

Status code: 200

Successful

```
{
  "password_policy" : {
    "minimum_password_length" : 8,
    "require_lowercase_characters" : true,
    "require_numbers" : true,
    "require_symbols" : true,
    "require_uppercase_characters" : true,
    "password_reuse_prevention" : 1
  }
}
```

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.17.2 Updating Custom Password Policies

Function

This API is used to update custom password policies. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

PUT /v1/identity-stores/{identity_store_id}/password-policy

Table 4-893 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Request Parameters

Table 4-894 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Table 4-895 Parameters in the request body

Parameter	Mandatory	Type	Description
password_policy	Yes	**PasswordPolicyDto** object	

Table 4-896 PasswordPolicyDto

Parameter	Mandatory	Type	Description
minimum_password_length	No	Integer	Minimum password length.
require_lowercase_characters	No	Boolean	Whether lowercase letters are required.
require_numbers	No	Boolean	Whether digits are required.
require_symbols	No	Boolean	Whether special characters are required.
require_uppercase_characters	No	Boolean	Whether uppercase letters are required.
max_password_age	No	Integer	Password validity period.

Parameter	Mandatory	Type	Description
password_reuse_prevention	No	Integer	Password reuse limit. The default value is 1.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-897 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-898 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Updating custom password policies

```
PUT https://{hostname}/v1/identity-stores/{identity_store_id}/password-policy

{
  "password_policy" : {
    "minimum_password_length" : 8,
    "require_lowercase_characters" : true,
    "require_numbers" : true,
    "require_symbols" : true,
    "require_uppercase_characters" : true,
    "max_password_age" : 80,
    "password_reuse_prevention" : 1
```



```
  }
}
```

Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.18 SCIM User Management

4.18.1 Creating a User

Function

This API is used to synchronize a user to IAM Identity Center using the System for Cross-domain Identity Management (SCIM) protocol.

URI

POST /{tenant_id}/scim/v2/Users

Table 4-899 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant.

Request Parameters

Table 4-900 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token.

Table 4-901 Parameters in the request body

Parameter	Mandatory	Type	Description
externalId	No	String	External ID.
userName	Yes	String	Username, which uniquely identifies a user.
name	Yes	Object	User's name.
displayName	Yes	String	Display name of a user.
nickName	No	String	Nickname of a user.
profileUrl	No	String	URL associated with a user.
emails	Yes	Array of objects	Email addresses of a user.
addresses	No	Array of objects	Addresses of a user.
phoneNumbers	No	Array of objects	Phone numbers of a user.
userType	No	String	User type.
title	No	String	User title.
preferredLanguage	No	String	User's preferred language.
locale	No	String	Geographical area or location of a user.
timezone	No	String	Time zone of a user.
active	No	Boolean	Whether a user is enabled.
schemas	Yes	Array of strings	Summary.
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User	No	Object	User work information.

Table 4-902 name

Parameter	Mandatory	Type	Description
formatted	No	String	Formatted name to be displayed.
familyName	Yes	String	Family name of a user.
givenName	Yes	String	Given name of a user.
middleName	No	String	Middle name of a user.
honorificPrefix	No	String	Prefix of a user's name.
honorificSuffix	No	String	Suffix of a user's name.

Table 4-903 emails

Parameter	Mandatory	Type	Description
value	Yes	String	Email address.
type	Yes	String	Email address type.
primary	Yes	Boolean	Whether the value is the user's primary email address.

Table 4-904 addresses

Parameter	Mandatory	Type	Description
formatted	No	String	Formatted address to be displayed.
streetAddress	No	String	Street.
locality	No	String	Location.
region	No	String	Region.
postalCode	No	String	Postal code.
country	No	String	Country or region.
type	No	String	Address type.
primary	No	Boolean	Whether the address is the user's primary address.

Table 4-905 phoneNumbers

Parameter	Mandatory	Type	Description
value	No	String	Phone number.
type	No	String	Phone number type.
primary	No	Boolean	Whether the value is the user's primary phone number.

Table 4-906 urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Parameter	Mandatory	Type	Description
costCenter	No	String	Cost Center. Minimum length: **1** Maximum length: **1024**
department	No	String	Department. Minimum length: **1** Maximum length: **1024**
division	No	String	Division. Minimum length: **1** Maximum length: **1024**
employeeNumber	No	String	Employee ID. Minimum length: **1** Maximum length: **1024**
manager	No	Object	Manager.
organization	No	String	Organization. Minimum length: **1** Maximum length: **1024**

Table 4-907 manager

Parameter	Mandatory	Type	Description
value	No	String	Manager. Minimum length: **1** Maximum length: **1024**

Response Parameters

Status code: 201

Table 4-908 Parameters in the response body

Parameter	Type	Description
id	String	Globally unique ID of a user.
externalId	String	External ID.
meta	Object	Metadata.
schemas	Array of strings	Summary.
userName	String	Username, which uniquely identifies a user.
name	Object	User's name.
displayName	String	Display name of a user.
nickName	String	Nickname of a user.
title	String	User title.
userType	String	User type.
preferredLanguage	String	User's preferred language.
locale	String	Geographical area or location of a user.
timezone	String	Time zone of a user.
active	Boolean	Whether a user is enabled.
emails	Array of objects	Email addresses of a user.
addresses	Array of objects	Addresses of a user.
phoneNumbers	Array of objects	Phone numbers of a user.
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User	Object	User work information.

Table 4-909 meta

Parameter	Type	Description
resourceType	String	Resource type.
created	String	Resource creation time.
lastModified	String	Last resource update time.

Table 4-910 name

Parameter	Type	Description
formatted	String	Formatted name to be displayed.
familyName	String	Family name of a user.
givenName	String	Given name of a user.
middleName	String	Middle name of a user.
honorificPrefix	String	Prefix of a user's name.
honorificSuffix	String	Suffix of a user's name.

Table 4-911 emails

Parameter	Type	Description
value	String	Email address.
type	String	Email address type.
primary	Boolean	Whether the value is the user's primary email address.

Table 4-912 addresses

Parameter	Type	Description
formatted	String	Formatted address to be displayed.
streetAddress	String	Street.
locality	String	Location.
region	String	Region.
postalCode	String	Postal code.

Parameter	Type	Description
country	String	Country or region.
type	String	Address type.
primary	Boolean	Whether the address is the user's primary address.

Table 4-913 phoneNumbers

Parameter	Type	Description
value	String	Phone number.
type	String	Phone number type.
primary	Boolean	Whether the value is the user's primary phone number.

Table 4-914 urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Parameter	Type	Description
costCenter	String	Cost Center. Minimum length: **1** Maximum length: **1024**
department	String	Department. Minimum length: **1** Maximum length: **1024**
division	String	Division. Minimum length: **1** Maximum length: **1024**
employeeNumber	String	Employee ID. Minimum length: **1** Maximum length: **1024**
manager	Object	Manager.
organization	String	Organization. Minimum length: **1** Maximum length: **1024**

Table 4-915 manager

Parameter	Type	Description
value	String	Manager. Minimum length: **1** Maximum length: **1024**

Status code: 400

Table 4-916 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 403

Table 4-917 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 404

Table 4-918 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.

Parameter	Type	Description
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 409

Table 4-919 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 500

Table 4-920 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Example Request

Creating a user

```
POST https://{hostname}/{tenant_id}/scim/v2/Users

{
```



```
  "externalId" : "123456",
  "userName" : "xxx",
  "name" : {
    "formatted" : "xxx",
    "familyName" : "xxx",
    "givenName" : "xxx",
    "middleName" : "xxx",
    "honorificPrefix" : "xxx",
    "honorificSuffix" : "xxx"
  },
  "displayName" : "xxx",
  "nickName" : "xxx",
  "profileUrl" : "xxx",
  "emails" : [ {
    "value" : "xxx",
    "type" : "work",
    "primary" : true
  } ],
  "addresses" : [ {
    "formatted" : "xxx",
    "streetAddress" : "xxx",
    "locality" : "xxx",
    "region" : "xxx",
    "postalCode" : "123456",
    "country" : "xxx",
    "type" : "work",
    "primary" : true
  } ],
  "phoneNumbers" : [ {
    "value" : "xxx",
    "type" : "work",
    "primary" : true
  } ],
  "userType" : "xxx",
  "title" : "xxx",
  "preferredLanguage" : "zh-CN",
  "locale" : "zh-CN",
  "timezone" : "xxx",
  "active" : true,
  "schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ]
}
```

Example Response

Status code: 201

Successful

```
{
  "id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
  "externalId" : "123456",
  "meta" : {
    "resourceType" : "User",
    "created" : "2023-04-08T14:53:43Z",
    "lastModified" : "2023-04-08T14:53:43Z"
  },
  "schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
  "userName" : "xxx",
  "name" : {
    "formatted" : "xxx",
    "familyName" : "xxx",
    "givenName" : "xxx",
    "middleName" : "xxx",
    "honorificPrefix" : "xxx",
    "honorificSuffix" : "xxx"
  },
  "displayName" : "xxx",
  "nickName" : "xxx",
  "title" : "xxx",
```



```
 "userType" : "xxx",
 "preferredLanguage" : "zh-CN",
 "locale" : "zh-CN",
 "timezone" : "xxx",
 "active" : true,
 "emails" : [ {
   "value" : "xxx",
   "type" : "work",
   "primary" : true
 } ],
 "addresses" : [ {
   "formatted" : "xxx",
   "streetAddress" : "xxx",
   "locality" : "xxx",
   "region" : "xxx",
   "postalCode" : "123456",
   "country" : "xxx",
   "type" : "work",
   "primary" : true
 } ],
 "phoneNumbers" : [ {
   "value" : "xxx",
   "type" : "work",
   "primary" : true
 } ]
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.18.2 Listing Users

Function

This API is used to list users. A maximum of 50 results can be returned for each request.

URI

GET /{tenant_id}/scim/v2/Users

Table 4-921 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant.

Request Parameters

Table 4-922 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token.

Response Parameters

Status code: 200

Table 4-923 Parameters in the response body

Parameter	Type	Description
totalResults	Integer	Total results.
itemsPerPage	String	Number of elements on each page.
startIndex	String	Start index.
schemas	Array of strings	Summary.
Resources	Array of objects	List of user information.

Table 4-924 Resources

Parameter	Type	Description
id	String	Globally unique ID of a user.
externalId	String	External ID.
meta	Object	Metadata.
schemas	Array of strings	Summary.
userName	String	Username, which uniquely identifies a user.
name	Object	User's name.
displayName	String	Display name of a user.
active	Boolean	Whether a user is enabled.
emails	Array of objects	Email addresses of a user.
userType	String	User type.

Parameter	Type	Description
nickName	String	Nickname of a user. Minimum length: **1** Maximum length: **1024**
title	String	User title. Minimum length: **1** Maximum length: **1024**
preferredLanguage	String	User's preferred language. Minimum length: **1** Maximum length: **1024**
locale	String	Geographical area or location of a user. Minimum length: **1** Maximum length: **1024**
timezone	String	User time zone. Minimum length: **1** Maximum length: **1024**
addresses	Array of objects	Address list of a user. Array length: **1-1**
phoneNumbers	Array of objects	Phone number list of a user. Array length: **1-1**
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User	Object	User work information.

Table 4-925 Resources.meta

Parameter	Type	Description
resourceType	String	Resource type.
created	String	Resource creation time.
lastModified	String	Last resource update time.

Table 4-926 Resources.name

Parameter	Type	Description
formatted	String	Formatted name to be displayed.
familyName	String	Family name of a user.
givenName	String	Given name of a user.
middleName	String	Middle name of a user.
honorificPrefix	String	Prefix of a user's name.
honorificSuffix	String	Suffix of a user's name.

Table 4-927 Resources.emails

Parameter	Type	Description
value	String	Email address.
type	String	Email address type.
primary	Boolean	Whether the value is the user's primary email address.

Table 4-928 users.addresses

Parameter	Type	Description
formatted	String	Formatted address to be displayed. Minimum length: **1** Maximum length: **1024**
streetAddress	String	Street. Minimum length: **1** Maximum length: **1024**
locality	String	Location. Minimum length: **1** Maximum length: **1024**
region	String	Region. Minimum length: **1** Maximum length: **1024**

Parameter	Type	Description
postalCode	String	Postal code. Minimum length: **1** Maximum length: **1024**
country	String	Country or region. Minimum length: **1** Maximum length: **1024**
type	String	Address type. Minimum length: **1** Maximum length: **1024**
primary	Boolean	Whether the address is the user's primary address.

Table 4-929 users.phoneNumbers

Parameter	Type	Description
value	String	Phone number. Minimum length: **1** Maximum length: **1024**
type	String	Phone number type. Minimum length: **1** Maximum length: **1024**
primary	Boolean	Whether the value is the user's primary phone number.

Table 4-930 urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Parameter	Type	Description
costCenter	String	Cost Center. Minimum length: **1** Maximum length: **1024**
department	String	Department. Minimum length: **1** Maximum length: **1024**

Parameter	Type	Description
division	String	Division. Minimum length: **1** Maximum length: **1024**
employeeNumber	String	Employee ID. Minimum length: **1** Maximum length: **1024**
manager	Object	Manager.
organization	String	Organization. Minimum length: **1** Maximum length: **1024**

Table 4-931 manager

Parameter	Type	Description
value	String	Manager. Minimum length: **1** Maximum length: **1024**

Status code: 400

Table 4-932 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 403

Table 4-933 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 404

Table 4-934 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 409

Table 4-935 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 500

Table 4-936 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Example Request

Listing users

```
GET https://{hostname}/{tenant_id}/scim/v2/Users
```

Example Response

Status code: 200

Successful

```
{
  "totalResults" : 1,
  "itemsPerPage" : 10,
  "startIndex" : "649040aaaaaaaaaaa3e3050",
  "schemas" : [ "urn:ietf:params:scim:api:messages:2.0:ListResponse" ],
  "Resources" : [ {
    "id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
    "externalId" : "123456",
    "meta" : {
      "resourceType" : "User",
      "created" : "2023-04-08T14:53:43Z",
      "lastModified" : "2023-04-08T14:53:43Z"
    },
    "schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
    "userName" : "xxx",
    "name" : {
      "formatted" : "xxx",
      "familyName" : "xxx",
      "givenName" : "xxx",
      "middleName" : "xxx",
      "honorificPrefix" : "xxx",
      "honorificSuffix" : "xxx"
    },
    "displayName" : "xxx",
    "active" : true,
    "emails" : [ {
      "value" : "xxx",
      "type" : "work",
      "primary" : true
    } ],
    "userType" : "xxx"
  } ]
}
```


Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.18.3 Querying User Details

Function

This API is used to query user details.

URI

GET /{tenant_id}/scim/v2/Users/{user_id}

Table 4-937 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant
user_id	Yes	String	Globally unique ID of a user

Request Parameters

Table 4-938 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Response Parameters

Status code: 200

Table 4-939 Parameters in the response body

Parameter	Type	Description
id	String	Globally unique ID of a user
externalId	String	External ID
meta	Object	Metadata
schemas	Array of strings	Summary

Parameter	Type	Description
userName	String	Username, which uniquely identifies a user
name	Object	Name of a user
displayName	String	Display name of a user
active	Boolean	Whether a user is enabled
emails	Array of objects	Email addresses of a user
userType	String	User type
nickName	String	Nickname of a user Minimum length: **1** Maximum length: **1024**
title	String	User title Minimum length: **1** Maximum length: **1024**
preferredLanguage	String	User's preferred language Minimum length: **1** Maximum length: **1024**
locale	String	Geographical area or location of a user Minimum length: **1** Maximum length: **1024**
timezone	String	User time zone Minimum length: **1** Maximum length: **1024**
addresses	Array of objects	Address list of a user Array length: **1-1**
phoneNumbers	Array of objects	Phone number list of a user Array length: **1-1**
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User	Object	Object that contains the user's work-related information

Table 4-940 meta

Parameter	Type	Description
resourceType	String	Resource type
created	String	Resource creation time
lastModified	String	Last resource update time

Table 4-941 name

Parameter	Type	Description
formatted	String	Formatted name to be displayed
familyName	String	Family name of a user
givenName	String	Given name of a user
middleName	String	Middle name of a user
honorificPrefix	String	Prefix of a user name
honorificSuffix	String	Suffix of a user name

Table 4-942 emails

Parameter	Type	Description
value	String	Email address
type	String	Email address type
primary	Boolean	Whether the value is the user's primary email address

Table 4-943 users.addresses

Parameter	Type	Description
formatted	String	Formatted address to be displayed Minimum length: **1** Maximum length: **1024**
streetAddress	String	Street Minimum length: **1** Maximum length: **1024**

Parameter	Type	Description
locality	String	Locality Minimum length: **1** Maximum length: **1024**
region	String	Region Minimum length: **1** Maximum length: **1024**
postalCode	String	Postal code Minimum length: **1** Maximum length: **1024**
country	String	Country or region Minimum length: **1** Maximum length: **1024**
type	String	Address type Minimum length: **1** Maximum length: **1024**
primary	Boolean	Whether the address is the user's primary address

Table 4-944 users.phoneNumbers

Parameter	Type	Description
value	String	Phone number Minimum length: **1** Maximum length: **1024**
type	String	Phone number type Minimum length: **1** Maximum length: **1024**
primary	Boolean	Whether the value is the user's primary phone number

Table 4-945 urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Parameter	Type	Description
costCenter	String	Cost center Minimum length: **1** Maximum length: **1024**
department	String	Department Minimum length: **1** Maximum length: **1024**
division	String	Division Minimum length: **1** Maximum length: **1024**
employeeNumber	String	Employee ID Minimum length: **1** Maximum length: **1024**
manager	Object	Manager
organization	String	Organization Minimum length: **1** Maximum length: **1024**

Table 4-946 manager

Parameter	Type	Description
value	String	Manager Minimum length: **1** Maximum length: **1024**

Status code: 400

Table 4-947 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code

Parameter	Type	Description
timeStamp	String	Timestamp

Status code: 403

Table 4-948 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 404

Table 4-949 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 409

Table 4-950 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details

Parameter	Type	Description
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 500

Table 4-951 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Example Request

Querying user details

```
GET https://{hostname}/{tenant_id}/scim/v2/Users/{user_id}
```

Example Response

Status code: 200

Successful

```
{
  "id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
  "externalId" : "123456",
  "meta" : {
    "resourceType" : "User",
    "created" : "2023-04-08T14:53:43Z",
    "lastModified" : "2023-04-08T14:53:43Z"
  },
  "schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
  "userName" : "xxx",
  "name" : {
    "formatted" : "xxx",
    "familyName" : "xxx",
    "givenName" : "xxx",
    "middleName" : "xxx",
    "honorificPrefix" : "xxx",
    "honorificSuffix" : "xxx"
  },
  "displayName" : "xxx",
  "active" : true,
  "emails" : [ {
    "value" : "xxx",
    "type" : "work",
```



```
    "primary" : true
  } ],
  "userType" : "xxx"
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.18.4 Deleting a User

Function

This API is used to delete a user.

URI

DELETE /{tenant_id}/scim/v2/Users/{user_id}

Table 4-952 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant
user_id	Yes	String	Globally unique ID of a user

Request Parameters

Table 4-953 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Response Parameters

Status code: 400

Table 4-954 Parameters in the response body

Parameter	Type	Description
schema	String	Summary

Parameter	Type	Description
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 403

Table 4-955 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 404

Table 4-956 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 409

Table 4-957 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 500

Table 4-958 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Example Request

Deleting a user

```
DELETE https://{hostname}/{tenant_id}/scim/v2/Users/{user_id}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.18.5 Updating a User

Function

This API is used to update a user.

URI

PUT /{tenant_id}/scim/v2/Users/{user_id}

Table 4-959 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant.
user_id	Yes	String	Globally unique ID of a user.

Request Parameters

Table 4-960 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token.

Table 4-961 Parameters in the request body

Parameter	Mandatory	Type	Description
id	No	String	Globally unique ID of a user.
externalId	No	String	External ID.
userName	Yes	String	Username, which uniquely identifies a user.
name	Yes	Object	User's name.
displayName	Yes	String	Display name of a user.
nickName	No	String	Nickname of a user.
profileUrl	No	String	URL associated with a user.
emails	Yes	Array of objects	Email addresses of a user.
addresses	No	Array of objects	Addresses of a user.

Parameter	Mandatory	Type	Description
phoneNumbers	No	Array of objects	Phone numbers of a user.
userType	No	String	User type.
title	No	String	User title.
preferredLanguage	No	String	User's preferred language.
locale	No	String	Geographical area or location of a user.
timezone	No	String	Time zone of a user.
active	No	Boolean	Whether a user is enabled.
schemas	Yes	Array of strings	Summary.
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User	No	Object	User work information.

Table 4-962 name

Parameter	Mandatory	Type	Description
formatted	No	String	Formatted name to be displayed.
familyName	Yes	String	Family name of a user.
givenName	Yes	String	Given name of a user.
middleName	No	String	Middle name of a user.
honorificPrefix	No	String	Prefix of a user's name.
honorificSuffix	No	String	Suffix of a user's name.

Table 4-963 emails

Parameter	Mandatory	Type	Description
value	Yes	String	Email address.

Parameter	Mandatory	Type	Description
type	Yes	String	Email address type.
primary	Yes	Boolean	Whether the value is the user's primary email address.

Table 4-964 addresses

Parameter	Mandatory	Type	Description
formatted	No	String	Formatted address to be displayed.
streetAddress	No	String	Street.
locality	No	String	Location.
region	No	String	Region.
postalCode	No	String	Postal code.
country	No	String	Country or region.
type	No	String	Address type.
primary	No	Boolean	Whether the address is the user's primary address.

Table 4-965 phoneNumbers

Parameter	Mandatory	Type	Description
value	No	String	Phone number.
type	No	String	Phone number type.
primary	No	Boolean	Whether the value is the user's primary phone number.

Table 4-966 urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Parameter	Mandatory	Type	Description
costCenter	No	String	Cost Center. Minimum length: **1** Maximum length: **1024**

Parameter	Mandatory	Type	Description
department	No	String	Department. Minimum length: **1** Maximum length: **1024**
division	No	String	Division. Minimum length: **1** Maximum length: **1024**
employeeNumber	No	String	Employee ID. Minimum length: **1** Maximum length: **1024**
manager	No	Object	Manager.
organization	No	String	Organization. Minimum length: **1** Maximum length: **1024**

Table 4-967 manager

Parameter	Mandatory	Type	Description
value	No	String	Manager. Minimum length: **1** Maximum length: **1024**

Response Parameters

Status code: 200

Table 4-968 Parameters in the response body

Parameter	Type	Description
id	String	Globally unique ID of a user.
externalId	String	External ID.
meta	Object	Metadata.
schemas	Array of strings	Summary.
userName	String	Username, which uniquely identifies a user.
name	Object	User's name.

Parameter	Type	Description
displayName	String	Display name of a user.
nickName	String	Nickname of a user.
title	String	User title.
userType	String	User type.
preferredLanguage	String	User's preferred language.
locale	String	Geographical area or location of a user.
timezone	String	Time zone of a user.
active	Boolean	Whether a user is enabled.
emails	Array of objects	Email addresses of a user.
addresses	Array of objects	Addresses of a user.
phoneNumbers	Array of objects	Phone numbers of a user.
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User	Object	User work information.

Table 4-969 meta

Parameter	Type	Description
resourceType	String	Resource type.
created	String	Resource creation time.
lastModified	String	Last resource update time.

Table 4-970 name

Parameter	Type	Description
formatted	String	Formatted name to be displayed.
familyName	String	Family name of a user.
givenName	String	Given name of a user.

Parameter	Type	Description
middleName	String	Middle name of a user.
honorificPrefix	String	Prefix of a user's name.
honorificSuffix	String	Suffix of a user's name.

Table 4-971 emails

Parameter	Type	Description
value	String	Email address.
type	String	Email address type.
primary	Boolean	Whether the value is the user's primary email address.

Table 4-972 addresses

Parameter	Type	Description
formatted	String	Formatted address to be displayed.
streetAddress	String	Street.
locality	String	Location.
region	String	Region.
postalCode	String	Postal code.
country	String	Country or region.
type	String	Address type.
primary	Boolean	Whether the address is the user's primary address.

Table 4-973 phoneNumbers

Parameter	Type	Description
value	String	Phone number.
type	String	Phone number type.
primary	Boolean	Whether the value is the user's primary phone number.

Table 4-974 urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Parameter	Type	Description
costCenter	String	Cost Center. Minimum length: **1** Maximum length: **1024**
department	String	Department. Minimum length: **1** Maximum length: **1024**
division	String	Division. Minimum length: **1** Maximum length: **1024**
employeeNumber	String	Employee ID. Minimum length: **1** Maximum length: **1024**
manager	Object	Manager.
organization	String	Organization. Minimum length: **1** Maximum length: **1024**

Table 4-975 manager

Parameter	Type	Description
value	String	Manager. Minimum length: **1** Maximum length: **1024**

Status code: 400

Table 4-976 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.

Parameter	Type	Description
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 403

Table 4-977 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 404

Table 4-978 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 409

Table 4-979 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.

Parameter	Type	Description
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 500

Table 4-980 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Example Request

Updating a user

```
PUT https://{hostname}/{tenant_id}/scim/v2/Users/{user_id}

{
  "id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
  "externalId" : "123456",
  "userName" : "xxx",
  "name" : {
    "formatted" : "xxx",
    "familyName" : "xxx",
    "givenName" : "xxx",
    "middleName" : "xxx",
    "honorificPrefix" : "xxx",
    "honorificSuffix" : "xxx"
  },
  "displayName" : "xxx",
  "nickName" : "xxx",
  "profileUrl" : "xxx",
  "emails" : [ {
    "value" : "xxx",
    "type" : "work",
    "primary" : true
  } ],
  "addresses" : [ {
    "formatted" : "xxx",
    "streetAddress" : "xxx",
    "locality" : "xxx",
```



```
    "region" : "xxx",
    "postalCode" : "123456",
    "country" : "xxx",
    "type" : "work",
    "primary" : true
  } ],
  "phoneNumbers" : [ {
    "value" : "xxx",
    "type" : "work",
    "primary" : true
  } ],
  "userType" : "xxx",
  "title" : "xxx",
  "preferredLanguage" : "zh-CN",
  "locale" : "zh-CN",
  "timezone" : "xxx",
  "active" : true,
  "schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ]
}
```

Example Response

Status code: 201

Successful

```
{
  "id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
  "externalId" : "123456",
  "meta" : {
    "resourceType" : "User",
    "created" : "2023-04-08T14:53:43Z",
    "lastModified" : "2023-04-16T21:32:55Z"
  },
  "schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
  "userName" : "xxx",
  "name" : {
    "formatted" : "xxx",
    "familyName" : "xxx",
    "givenName" : "xxx",
    "middleName" : "xxx",
    "honorificPrefix" : "xxx",
    "honorificSuffix" : "xxx"
  },
  "displayName" : "xxx",
  "nickName" : "xxx",
  "title" : "xxx",
  "userType" : "xxx",
  "preferredLanguage" : "zh-CN",
  "locale" : "zh-CN",
  "timezone" : "xxx",
  "active" : true,
  "emails" : [ {
    "value" : "xxx",
    "type" : "work",
    "primary" : true
  } ],
  "addresses" : [ {
    "formatted" : "xxx",
    "streetAddress" : "xxx",
    "locality" : "xxx",
    "region" : "xxx",
    "postalCode" : "123456",
    "country" : "xxx",
    "type" : "work",
    "primary" : true
  } ],
  "phoneNumbers" : [ {
    "value" : "xxx",
```



```
    "type" : "work",
    "primary" : true
  } ]
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.18.6 Partially Updating a User

Function

This API is used to update some attributes of a user.

URI

PATCH /{tenant_id}/scim/v2/Users/{user_id}

Table 4-981 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant
user_id	Yes	String	Globally unique ID of a user

Request Parameters

Table 4-982 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Table 4-983 Parameters in the request body

Parameter	Mandatory	Type	Description
schemas	Yes	Array of strings	Summary
Operations	Yes	Array of objects	List of the updates to be performed

Table 4-984 Operations

Parameter	Mandatory	Type	Description
op	Yes	String	Update type. **add**: add an attribute; **replace**: replace an attribute; **remove**: remove an attribute.
path	No	String	Attribute path to be updated. Only the following attributes of a user can be updated: userName, active, externalId, displayName, nickName, title, userType, preferredLanguage, locale, timezone, name, enterprise, emails, addresses, and phoneNumbers.
value	No	Object	Attribute value to be updated. You do not need to set this parameter if you intend to remove an attribute.

Response Parameters

Status code: 200

Table 4-985 Parameters in the response body

Parameter	Type	Description
id	String	Globally unique ID of a user
externalId	String	External ID
meta	Object	Metadata
schemas	Array of strings	Summary
userName	String	Username, which uniquely identifies a user
name	Object	Name of a user
displayName	String	Display name of a user
nickName	String	Nickname of a user
title	String	User title
userType	String	User type
preferredLanguage	String	User's preferred language

Parameter	Type	Description
locale	String	Geographical area or location of a user
timezone	String	Time zone of a user
active	Boolean	Whether a user is enabled
emails	Array of objects	Email addresses of a user
addresses	Array of objects	Addresses of a user
phoneNumbers	Array of objects	Phone numbers of a user
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User	Object	User's work-related information

Table 4-986 meta

Parameter	Type	Description
resourceType	String	Resource type
created	String	Resource creation time
lastModified	String	Last resource update time

Table 4-987 name

Parameter	Type	Description
formatted	String	Formatted name to be displayed
familyName	String	Family name of a user
givenName	String	Given name of a user
middleName	String	Middle name of a user
honorificPrefix	String	Prefix of a user name
honorificSuffix	String	Suffix of a user name

Table 4-988 emails

Parameter	Type	Description
value	String	Email address
type	String	Email address type
primary	Boolean	Whether the value is the user's primary email address

Table 4-989 addresses

Parameter	Type	Description
formatted	String	Formatted address to be displayed
streetAddress	String	Street
locality	String	Location
region	String	Region
postalCode	String	Postal code
country	String	Country or region
type	String	Address type
primary	Boolean	Whether the address is the user's primary address

Table 4-990 phoneNumbers

Parameter	Type	Description
value	String	Phone number
type	String	Phone number type
primary	Boolean	Whether the value is the user's primary phone number

Table 4-991 urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Parameter	Type	Description
costCenter	String	Cost center Minimum length: **1** Maximum length: **1024**

Parameter	Type	Description
department	String	Department Minimum length: **1** Maximum length: **1024**
division	String	Division Minimum length: **1** Maximum length: **1024**
employeeNumber	String	Employee ID Minimum length: **1** Maximum length: **1024**
manager	Object	Manager
organization	String	Organization Minimum length: **1** Maximum length: **1024**

Table 4-992 manager

Parameter	Type	Description
value	String	Manager Minimum length: **1** Maximum length: **1024**

Status code: 400

Table 4-993 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 403

Table 4-994 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 404

Table 4-995 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 409

Table 4-996 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 500

Table 4-997 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Example Request

Updating some attributes of an existing user

```
PATCH https://{hostname}/{tenant_id}/scim/v2/Users/{user_id}

{
  "schemas" : [ "urn:ietf:params:scim:api:messages:2.0:PatchOp" ],
  "Operations" : [ {
    "op" : "replace",
    "path" : "active",
    "value" : "false"
  } ]
}
```

Example Response

Status code: 200

Successful

```
{
  "id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
  "externalId" : "123456",
  "meta" : {
    "resourceType" : "User",
    "created" : "2023-04-08T14:53:43Z",
    "lastModified" : "2023-04-16T21:32:55Z"
  },
  "schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
  "userName" : "xxx",
  "name" : {
    "formatted" : "xxx",
    "familyName" : "xxx",
    "givenName" : "xxx",
    "middleName" : "xxx",
    "honorificPrefix" : "xxx",
    "honorificSuffix" : "xxx"
  },
  "displayName" : "xxx",
  "nickName" : "xxx",
  "title" : "xxx",
  "userType" : "xxx",
  "preferredLanguage" : "zh-CN",
  "locale" : "zh-CN",
  "timezone" : "xxx",
  "active" : false,
  "emails" : [ {
```



```
    "value" : "xxx",
    "type" : "work",
    "primary" : true
  } ],
  "addresses" : [ {
    "formatted" : "xxx",
    "streetAddress" : "xxx",
    "locality" : "xxx",
    "region" : "xxx",
    "postalCode" : "123456",
    "country" : "xxx",
    "type" : "xxx",
    "primary" : true
  } ],
  "phoneNumbers" : [ {
    "value" : "xxx",
    "type" : "work",
    "primary" : true
  } ]
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.19 SCIM Group Management

4.19.1 Creating a Group

Function

This API is used to synchronize a group to IAM Identity Center using the SCIM protocol.

URI

POST /{tenant_id}/scim/v2/Groups

Table 4-998 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant

Request Parameters

Table 4-999 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Table 4-1000 Parameters in the request body

Parameter	Mandatory	Type	Description
externalId	No	String	External ID
displayName	Yes	String	Display name of a group
members	No	Array of objects	List of member objects in a group
schemas	Yes	Array of strings	Summary

Table 4-1001 members

Parameter	Mandatory	Type	Description
value	Yes	String	Globally unique ID of a member
$ref	No	String	Reference information of a member
type	No	String	Member type. **User**: user

Response Parameters

Status code: 201

Table 4-1002 Parameters in the response body

Parameter	Type	Description
id	String	Globally unique ID of a group
externalId	String	External ID
meta	Object	Metadata
schemas	Array of strings	Summary

Parameter	Type	Description
displayName	String	Display name of a group
members	Array of objects	Members in a group

Table 4-1003 meta

Parameter	Type	Description
resourceType	String	Resource type
created	String	Resource creation time
lastModified	String	Last resource update time

Table 4-1004 members

Parameter	Type	Description
value	String	Globally unique ID of a member
$ref	String	Reference information of a member
type	String	Member type. **User**: user

Status code: 400

Table 4-1005 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 403

Table 4-1006 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 404

Table 4-1007 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 409

Table 4-1008 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 500

Table 4-1009 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Example Request

Creating a group

```
POST https://{hostname}/{tenant_id}/scim/v2/Groups

{
  "displayName" : "SCIM group name g1",
  "members" : [ {
    "value" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
    "$ref" : "../Users/ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
    "type" : "User"
  } ],
  "schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:Group" ]
}
```

Example Response

Status code: 201

Successful

```
{
  "id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
  "meta" : {
    "resourceType" : "Group",
    "created" : "2023-04-08T14:53:43Z",
    "lastModified" : "2023-04-08T14:53:43Z"
  },
  "schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:Group" ],
  "displayName" : "SCIM group name g1",
  "members" : [ {
    "value" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
    "$ref" : "../Users/ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
    "type" : "User"
  } ]
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.19.2 Listing Groups

Function

This API is used to list groups. A maximum of 50 results can be returned for each request.

URI

GET /{tenant_id}/scim/v2/Groups

Table 4-1010 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant.

Request Parameters

Table 4-1011 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token.

Response Parameters

Status code: 200

Table 4-1012 Parameters in the response body

Parameter	Type	Description
totalResults	Integer	Total results.
itemsPerPage	Integer	Number of elements on each page.
startIndex	String	Start index.
schemas	Array of strings	Summary.
Resources	Array of objects	List of group information.

Table 4-1013 Resources

Parameter	Type	Description
id	String	Globally unique ID of a group.
externalId	String	External ID.
meta	Object	Metadata.
schemas	Array of strings	Summary.
displayName	String	Display name of a group.
members	Array of objects	Members in a group.

Table 4-1014 Resources.meta

Parameter	Type	Description
resourceType	String	Resource type.
created	String	Resource creation time.
lastModified	String	Last resource update time.

Table 4-1015 Resources.members

Parameter	Type	Description
value	String	Globally unique ID of a member.
$ref	String	Reference information of a member.
type	String	Member type. **User**: user

Status code: 400

Table 4-1016 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.

Parameter	Type	Description
timeStamp	String	Timestamp.

Status code: 403

Table 4-1017 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 404

Table 4-1018 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 409

Table 4-1019 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.

Parameter	Type	Description
status	Integer	Status code.
timeStamp	String	Timestamp.

Status code: 500

Table 4-1020 Parameters in the response body

Parameter	Type	Description
schema	String	Summary.
schemas	Array of strings	Summary list.
detail	String	Exception details.
status	Integer	Status code.
timeStamp	String	Timestamp.

Example Request

Listing groups

```
GET https://{hostname}/{tenant_id}/scim/v2/Groups
```

Example Response

Status code: 200

Successful

```
{
  "totalResults" : 1,
  "itemsPerPage" : 10,
  "startIndex" : "649040aaaaaaaaaaa3e3050",
  "schemas" : [ "urn:ietf:params:scim:api:messages:2.0:ListResponse" ],
  "Resources" : [ {
    "id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
    "meta" : {
      "resourceType" : "Group",
      "created" : "2023-04-08T14:53:43Z",
      "lastModified" : "2023-04-08T14:53:43Z"
    },
    "schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:Group" ],
    "displayName" : "SCIM group name g1",
    "members" : [ {
      "value" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
      "$ref" : "../Users/ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
      "type" : "User"
    } ]
  } ]
}
```


Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.19.3 Querying Group Details

Function

This API is used to query group details.

URI

GET /{tenant_id}/scim/v2/Groups/{group_id}

Table 4-1021 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant
group_id	Yes	String	Globally unique ID of a group

Request Parameters

Table 4-1022 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Response Parameters

Status code: 200

Table 4-1023 Parameters in the response body

Parameter	Type	Description
id	String	Globally unique ID of a group
externalId	String	External ID
meta	Object	Metadata
schemas	Array of strings	Summary

Parameter	Type	Description
displayName	String	Display name of a group
members	Array of objects	Members in a group

Table 4-1024 meta

Parameter	Type	Description
resourceType	String	Resource type
created	String	Resource creation time
lastModified	String	Last resource update time

Table 4-1025 members

Parameter	Type	Description
value	String	Globally unique ID of a member
$ref	String	Reference information of a member
type	String	Member type. **User**: user

Status code: 400

Table 4-1026 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 403

Table 4-1027 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 404

Table 4-1028 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 409

Table 4-1029 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 500

Table 4-1030 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Example Request

Querying group details

```
GET https://{hostname}/{tenant_id}/scim/v2/Groups/{group_id}
```

Example Response

Status code: 200

Successful

```
{
  "id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
  "meta" : {
    "resourceType" : "Group",
    "created" : "2023-04-08T14:53:43Z",
    "lastModified" : "2023-04-08T14:53:43Z"
  },
  "schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:Group" ],
  "displayName" : "SCIM group name g1",
  "members" : [ {
    "value" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
    "$ref" : "../Users/ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9",
    "type" : "User"
  } ]
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.19.4 Deleting a Group

Function

This API is used to delete a group.

URI

DELETE /{tenant_id}/scim/v2/Groups/{group_id}

Table 4-1031 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant
group_id	Yes	String	Globally unique ID of a group

Request Parameters

Table 4-1032 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Response Parameters

Status code: 400

Table 4-1033 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 403

Table 4-1034 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list

Parameter	Type	Description
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 404

Table 4-1035 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 409

Table 4-1036 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 500

Table 4-1037 Parameters in the response body

Parameter	Type	Description
schema	String	Summary

Parameter	Type	Description
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Example Request

Deleting a group

```
DELETE https://{hostname}/{tenant_id}/scim/v2/Groups/{group_id}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.19.5 Partially Updating a Group

Function

This API is used to update some attributes of an existing group and manage users in the group.

URI

PATCH /{tenant_id}/scim/v2/Groups/{group_id}

Table 4-1038 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant
group_id	Yes	String	Globally unique ID of a group

Request Parameters

Table 4-1039 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Table 4-1040 Parameters in the request body

Parameter	Mandatory	Type	Description
schemas	Yes	Array of strings	Summary
Operations	Yes	Array of objects	List of the updates to be performed

Table 4-1041 Operations

Parameter	Mandatory	Type	Description
op	Yes	String	Update type. **add**: add an attribute; **replace**: replace an attribute; **remove**: remove an attribute.
value	No	Object	Attribute value to be updated
path	No	String	Attribute path to be updated. Only the following attributes of a group can be modified: displayName, members, and externalId.

Response Parameters

Status code: 400

Table 4-1042 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details

Parameter	Type	Description
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 403

Table 4-1043 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 404

Table 4-1044 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 409

Table 4-1045 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list

Parameter	Type	Description
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 500

Table 4-1046 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Example Request

Updating some attributes of a group

```
PATCH https://{hostname}/{tenant_id}/scim/v2/Groups/{group_id}

{
  "schemas" : [ "urn:ietf:params:scim:api:messages:2.0:PatchOp" ],
  "Operations" : [ {
    "op" : "replace",
    "value" : {
      "id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaf31a",
      "displayName" : "Update display name"
    }
  }, {
    "op" : "add",
    "path" : "members",
    "value" : [ {
      "value" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9"
    } ]
  }, {
    "op" : "replace",
    "path" : "members",
    "value" : [ {
      "value" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9"
    }, {
      "value" : "1bdaa75c-7aaf-3aa2-7aac-6a00aaaa335f"
    } ]
  }, {
    "op" : "remove",
    "path" : "members",
    "value" : [ {
      "value" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9"
    }, {
```



```
    "value" : "1bdaa75c-7aaf-3aa2-7aac-6a00aaaa335f"
  } ]
 } ]
}
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.20 Service Provider (SP) Management

4.20.1 Querying the SP Configuration

Function

This API is used to query the SCIM configuration in IAM Identity Center.

URI

GET /{tenant_id}/scim/v2/ServiceProviderConfig

Table 4-1047 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant

Request Parameters

Table 4-1048 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Response Parameters

Status code: 200

Table 4-1049 Parameters in the response body

Parameter	Type	Description
schemas	Array of strings	Summary
documentationUri	String	Help documentation URL
authenticationSchemes	Array of objects	List of authentication schemes
patch	Object	Whether an SP supports partial modifications and related configurations
bulk	Object	Whether an SP supports batch operations and related configurations
filter	Object	Whether an SP supports filtering and related configurations
changePassword	Object	Whether an SP supports the password change and related configurations
sort	Object	Whether an SP supports sorting and related configurations
etag	Object	Whether an SP supports electronic tags and related configurations

Table 4-1050 authenticationSchemes

Parameter	Type	Description
type	String	Authentication type
name	String	Name of an authentication scheme
description	String	Description of an authentication scheme
specUri	String	Specification URL
documentationUri	String	Help documentation URL
primary	Boolean	Whether the value is the primary authentication method

Table 4-1051 patch

Parameter	Type	Description
supported	Boolean	Whether an SP supports the operation

Table 4-1052 bulk

Parameter	Type	Description
supported	Boolean	Whether an SP supports the operation
maxOperations	Integer	Maximum number of operations that can be performed at a time
maxPayloadSize	Integer	Maximum valid payload

Table 4-1053 filter

Parameter	Type	Description
supported	Boolean	Whether an SP supports the operation
maxResults	Integer	Maximum number of results

Table 4-1054 changePassword

Parameter	Type	Description
supported	Boolean	Whether an SP supports the operation

Table 4-1055 sort

Parameter	Type	Description
supported	Boolean	Whether an SP supports the operation

Table 4-1056 etag

Parameter	Type	Description
supported	Boolean	Whether an SP supports the operation

Status code: 400

Table 4-1057 Parameters in the response body

Parameter	Type	Description
schema	String	Summary

Parameter	Type	Description
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 403

Table 4-1058 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 404

Table 4-1059 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 409

Table 4-1060 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Status code: 500

Table 4-1061 Parameters in the response body

Parameter	Type	Description
schema	String	Summary
schemas	Array of strings	Summary list
detail	String	Exception details
status	Integer	Status code
timeStamp	String	Timestamp

Example Request

Querying the SCIM configuration in IAM Identity Center

```
GET https://{hostname}/{tenant_id}/scim/v2/ServiceProviderConfig
```

Example Response

Status code: 200

Successful

```
{
  "schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:ServiceProviderConfig" ],
  "documentationUri" : null,
  "authenticationSchemes" : [ {
    "type" : "authenticationtype",
    "name" : "Authentication Name",
    "description" : "Authentication scheme using the AAA Authentication Standard",
    "specUri" : "http://www.example.org/doc/auth1234",
    "documentationUri" : null,
    "primary" : true
  } ],
  "patch" : {
    "supported" : false
```



```
  },
  "bulk" : {
    "supported" : false,
    "maxOperations" : null,
    "maxPayloadSize" : null
  },
  "filter" : {
    "supported" : false,
    "maxResults" : null
  },
  "changePassword" : {
    "supported" : false
  },
  "sort" : {
    "supported" : false
  },
  "etag" : {
    "supported" : false
  }
}
```


Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.20.2 Creating a Service Provider Certificate

Function

This API is used to create a SAML signing certificate of a service provider. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/saml-certificates

Table 4-1062 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Request Parameters

Table 4-1063 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 201

Table 4-1064 Parameters in the response body

Parameter	Type	Description
certificate_id	String	Certificate ID.
x509certificate	String	X.509 certificate.
algorithm	String	Signature algorithm.
expiry_date	Long	Certificate expiration timestamp.
state	String	Certificate activation status.

Status code: 400

Table 4-1065 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-1066 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Creating a SAML signing certificate of a service provider

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/saml-certificates
```

Example Response

Status code: 201

Successful

```
{
  "certificate_id" : "cer-89a0723d-fdfd-40cb-9fb6-14xxxx",
  "x509certificate" : "-----BEGIN CERTIFICATE-----\r\nMIIEzDCCAzSgAwIBAg**********OrPhEc=\r\n-----END CERTIFICATE-----",
  "algorithm" : "SHA256withRSA",
  "expiry_date" : 2069798400000,
  "state" : "INACTIVE"
}
```

Status Codes

Status Code	Description
201	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.20.3 Listing Service Provider Certificates

Function

This API is used to query the SAML signing certificate of a service provider.

URI

GET /v1/identity-stores/{identity_store_id}/saml-certificates

Table 4-1067 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Request Parameters

Table 4-1068 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-1069 Parameters in the response body

Parameter	Type	Description
Array	Array of SpCertificateDto objects	Details of a service provider certificate.

Table 4-1070 SpCertificateDto

Parameter	Type	Description
certificate_id	String	Certificate ID.
x509certificate	String	X.509 certificate.
algorithm	String	Signature algorithm.
expiry_date	Long	Certificate expiration timestamp.
state	String	Certificate activation status.

Status code: 400

Table 4-1071 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-1072 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying the SAML signing certificate of a service provider

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/saml-certificates
```

Example Response

Status code: 200

Successful

```
[ {
  "certificate_id" : "cer-6bea67d1-a875-4e63-b91f-c8081axxxx",
  "x509certificate" : "-----BEGIN CERTIFICATE-----\r\nMIIEzDCCAzSgAwIBAgICAdQwDQYJKoZIhv********O8=\r
\n-----END CERTIFICATE-----",
  "algorithm" : "SHA256withRSA",
  "expiry_date" : 2069798400000,
  "state" : "INACTIVE"
}, {
  "certificate_id" : "cer-89a0723d-fdfd-40cb-9fb6-148xxxxxx",
  "x509certificate" : "-----BEGIN CERTIFICATE-----\r\nMIIEzDCCAzSg********ODA0\r
\nMDAwMDAwWjCBqDEhMB8GA1UEAwwYaWRjZW50ZXIuaHVhd2VpY2xvdWQuY29tMSgwJgYDVQQLDB9T
\r\nZXJ2aWNlIFByb3ZpZGVyIE9wZXJhdGlvbiBEZXB0MSUwIwYDVQQKDBxIdWF3ZWkgVGVjaG5vbG9n\r
\naWVzIENvLiwgTHRkMREwDwYDVQQHDAhTaGVuWmhlbjESMBAGA1UECAwJR3VhbmdEb25nMQswCQYD
\r\nVQQGEwJDTjCCAaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBALFkWYIQXCYtJFQC+BpnaFwg\r\nT
+zH7E9cnplccR5Sk66zHYRIJdqITW7ZLhEDeVMy5whHxJ+gL+Fv4E0z82kH8nXa1QERdWYvbu54\r
\nnyOZopnQ0YhlIYLW6s7X3pDvxo1WMm7JlqEGuQoY7XF9+AdBeLv/kv2Jsb5g/F/pTZWc+a2ToX7k\r
\nqErPdNtbLSueDwpWacmOa/TDCXmrDM1DihX6Bw3/d/BsQnDglDCvYBlscgxv8IEDTqtL0Z7fpaGh\r
\nwGlia6wVqsl2C1nMeNijNzau3U9tvzzs0TyJ+I657yq2KD60cWBnjUaVAwrawf741Q9qZjfYFojP\r
\nFBoCkdLozNmlDZOFKHWuk81j/Z6JIZ4qEPkeFS+mjk/wBRVHYM5Tzj38XbMVvebQgykf3HKGlCwN\r
\nu5HzIftK8T9QVrF2OKYQNGplGt82aMA1fMhTMSW0pB6ab2byOdCOGrD7HoiThD8D680G4sPT+KkE\r
\nFsE3YkQRHNdSKb3efRULSqZpNGE44iOKzQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBgQALh5RknXV1\r
```


\nTEEXwVxF+6vMZ/+e9a54IS61vSwXHPf8rPA0e9vhhpONOxRb2nKQKygcwYAW98BVyjZ1v5INfFPo\r
\nTe5Zje8iM9sSNAxD6kUJifWzGhemu9Dv4tCnZUSlzPnffZkbxbUsyX5JngryQXZUiNMbRTV6IEt7\r
\niDQ8HaNaVXuGbQtZFA0kia78kkQd8p19C/TEIfI0YX6p+Kvhu13oq9TIBs+r9tfUoYsKsHYwF4gb\r
\nKKK3oNxq9VbNuZkLbLP20CNrcywMvnq81RklhA2kTkkgtb8IvoakLfnfCg6FbFrNfaqHOQ9lyrEh\r
\nZ5XzQFsqhCfR8eIYFPQ6rLDGPtrUVi/t27OTquAUjoCRHtuy44y+OKATKismvFvl+/LAb5wtNuWB\r
\nmpzYUFEBE7vVOdJfez9Sd5ujTtr1BDoVNfQ76eMo/p/EHtQjB0cfYnFv8SR9N9q4et0Oj15w4gZp\r
\n4XwzOATBm1A0G5blbbJjKGFU/RSVlNPA8UxkJudibOrPhEc=\r\n-----END CERTIFICATE-----",
  "algorithm" : "SHA256withRSA",
  "expiry_date" : 2069798400000,
  "state" : "INACTIVE"
}]

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.20.4 Deleting a Service Provider Certificate

Function

This API is used to delete a SAML signing certificate of a service provider. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

DELETE /v1/identity-stores/{identity_store_id}/saml-certificates/{certificate_id}

Table 4-1073 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
certificate_id	Yes	String	Globally unique ID of a certificate in the identity source.

Request Parameters

Table 4-1074 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful

Status code: 400

Table 4-1075 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-1076 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Deleting a SAML signing certificate of a service provider

```
DELETE https://{hostname}/v1/identity-stores/{identity_store_id}/saml-certificates/{certificate_id}
```


Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.20.5 Activating a Service Provider Certificate

Function

This API is used to activate a SAML signing certificate of a service provider. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

POST /v1/identity-stores/{identity_store_id}/saml-certificates/{certificate_id}/active

Table 4-1077 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.
certificate_id	Yes	String	Globally unique ID of a certificate in the identity source.

Request Parameters

Table 4-1078 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Successful.

Status code: 400

Table 4-1079 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-1080 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Activating a SAML signing certificate of a service provider

```
POST https://{hostname}/v1/identity-stores/{identity_store_id}/saml-certificates/{certificate_id}/active
```


Example Response

None

Status Codes

Status Code	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.20.6 Querying Service Provider Configurations

Function

This API is used to query service provider configurations. It can be called only from the organization's management account or from a delegated administrator account of a cloud service.

URI

GET /v1/identity-stores/{identity_store_id}/sp-config

Table 4-1081 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of an identity source.

Request Parameters

Table 4-1082 Parameters in the request header

Parameter	Mandatory	Type	Description
X-Security-Token	No	String	Security token (session token) of your temporary security credentials. If a temporary security credential is used, this header is required.

Response Parameters

Status code: 200

Table 4-1083 Parameters in the response body

Parameter	Type	Description
sp_oidc_config	**SPOIDCConfig** object	OIDC configuration of a service provider.
sp_saml_config	**SPSAMLConfig** object	SAML configuration of a service provider.

Table 4-1084 SPOIDCConfig

Parameter	Type	Description
redirect_url	String	Redirect URL.

Table 4-1085 SPSAMLConfig

Parameter	Type	Description
acs_url	String	Response address of a service provider's assertion.
issuer	String	Service provider issuer.
metadata	String	Service provider metadata.

Status code: 400

Table 4-1086 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.

Status code: 403

Table 4-1087 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
request_id	String	Unique ID of a request.
encoded_authorization_message	String	Encrypted error message.

Example Request

Querying service provider configurations

```
GET https://{hostname}/v1/identity-stores/{identity_store_id}/sp-config
```

Example Response

Status code: 200

Successful

```
{
  "sp_oidc_config" : {
    "redirect_url" : "https://cn-north-4.signin.huaweicloud.com/platform/oauth2/callback/xxxxx"
  },
  "sp_saml_config" : {
    "acs_url" : "https://cn-north-4-signin.huaweicloud.com/v1/platform/saml/acs/xxxxx",
    "issuer" : "https://cn-north-4.signin.huaweicloud.com/platform/saml/xxxxx",
    "metadata" : "<?xml version=\"1.0\" encoding=\"UTF-8\"?><md:EntityDescriptor xmlns:md=
\"urn:oasis:names:tc:SAML:2.0:metadata\" entityID=\"https:xxxxxx\">xxxxx</md:EntityDescriptor>"
  }
}
```

Status Codes

Status Codes	Description
200	Successful.
400	Bad request.
403	Forbidden.

Error Codes

For details, see **Error Codes**.

4.21 Client Management

4.21.1 Registering a Client

Function

This API is used to register a client in IAM Identity Center, which allows the client to initiate device authorization. The output should be persistent for reuse by authentication requests.

URI

POST /v1/clients

Request Parameters

Table 4-1088 Parameters in the request body

Parameter	Mandatory	Type	Description
client_name	Yes	String	Client name Minimum length: **1** Maximum length: **1024**
client_type	Yes	String	Client type. Only the public client is supported. Enumerated value: • **public**
token_endpoint_auth_method	Yes	String	Authentication method required to send a request to the token endpoint Enumerated value: • **client_secret_post**
scopes	No	Array of strings	List of scopes defined by a client to restrict permissions for access token authorization
grant_types	Yes	Array of strings	OAuth2.0 authorization type that a client can use at the token endpoint Enumerated value: • **urn:ietf:params:oauth:grant-type:device_code** • **authorization_code**
response_types	Yes	Array of strings	OAuth2.0 authorization type that a client can use at the authorization endpoint Enumerated value: • **code**

Response Parameters

Status code: 200

Table 4-1089 Parameters in the response body

Parameter	Type	Description
client_info	Object	Client registration information

Table 4-1090 client_info

Parameter	Type	Description
authorization_endpoint	String	Authorization endpoint requested from a client
client_id	String	Unique ID of a client application
client_id_issued_at	Long	Registration time of the client ID and secret key
client_secret	String	Secret string generated for the client to obtain authorization from services in subsequent calls
client_secret_expires_at	Long	Expiration time of the client ID and secret key
token_endpoint	String	Endpoint from which a client can obtain an access token
scopes	Array of strings	List of registered scopes for subsequent authorization of access tokens for a client

Example Request

Registering a client in IAM Identity Center

```
POST https://{hostname}/v1/clients

{
  "client_name" : "exampleClient",
  "client_type" : "public",
  "token_endpoint_auth_method" : "client_secret_post",
  "scopes" : [ "openid" ],
  "grant_types" : [ "authorization_code", "urn:ietf:params:oauth:grant-type:device_code"],
  "response_types" : [ "code" ]
}
```

Example Response

Status code: 200

Successful

```
{
  "client_info" : {
    "authorization_endpoint" : "https://example-region-oidc.examplehh.com:443/v1/authorize",
    "client_id" : "example_client_id",
    "client_id_issued_at" : 1677175760,
    "client_secret" : "example_client_secret",
    "client_secret_expires_at" : 1684951760,
    "token_endpoint" : "https://example-region-oidc.examplehh.com:443/v1/tokens",
    "scopes" : [ "openid" ]
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.22 Token Management

4.22.1 Creating a Token

Function

This API is used to create an access token.

URI

POST /v1/tokens

Request Parameters

Table 4-1091 Parameters in the request body

Parameter	Mandatory	Type	Description
client_id	Yes	String	Unique ID of the client
client_secret	Yes	String	Secret string generated for the client to obtain authorization from services in subsequent calls
code	No	String	Authorization code received from the authorization service. This parameter is required when executing an authorization request to obtain access to the token.

Parameter	Mandatory	Type	Description
device_code	No	String	Used only when the authorization type (**grant_type**) is the device code (**urn:ietf:params:oauth:grant-type:device_code**).
grant_type	Yes	String	Authorization type, which can be authorization code, device code, client credential, and refresh token Enumerated value: • **authorization_code** • **urn:ietf:params:oauth:grant-type:device_code**
redirect_uri	No	String	Application URL that will receive the authorization code. The user authorizes a service to send a request to this URL.
refresh_token	No	String	Refresh token, which can be used to obtain a new access token after the original access token expires
scopes	No	Array of strings	List of scopes defined by a client to restrict permissions for access token authorization

Response Parameters

Status code: 200

Table 4-1092 Parameters in the response body

Parameter	Type	Description
token_info	Object	Token information

Table 4-1093 token_info

Parameter	Type	Description
access_token	String	Opaque token used to access IAM Identity Center resources assigned to users
expires_in	Integer	Expiration time (in seconds) of an access token

Parameter	Type	Description
id_token	String	Opaque token used to identify a user
refresh_token	String	Refresh token, which can be used to obtain a new access token after the original access token expires
token_type	String	Used to notify the client that the returned token is an access token. The value is **BearerToken** currently.

Example Request

Creating an access token

```
POST https://{hostname}/v1/tokens

{
  "client_id" : "example_client_id",
  "client_secret" : "example_client_secret",
  "code" : "1234567890123456",
  "device_code" : null,
  "grant_type" : "authorization_code",
  "redirect_uri" : "https://example-redirect.example.com/redirect/url",
  "refresh_token" : null,
  "scopes" : [ "openid" ]
}
```

Example Response

Status code: 200

Successful

```
{
  "token_info" : {
    "access_token" : "example_access_token",
    "expires_in" : 1684955360,
    "id_token" : "example_access_token",
    "refresh_token" : null,
    "token_type" : "Bearer"
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.23 Device Authorization Management

4.23.1 Requesting Device Authorization

Function

This API is used to request device authorization.

URI

POST /v1/device/authorize

Request Parameters

Table 4-1094 Parameters in the request body

Parameter	Mandatory	Type	Description
client_id	Yes	String	Unique ID of the client registered in the IAM Identity Center
client_secret	Yes	String	Secret string generated for the client to obtain authorization from services in subsequent calls
start_url	Yes	String	User Portal URL

Response Parameters

Status code: 200

Table 4-1095 Parameters in the response body

Parameter	Type	Description
device_code	String	Device code used by the device to poll session tokens
expires_in	Integer	Expiration time of a device code (in seconds)
interval	Integer	Number of seconds the client must wait for between two attempts when polling a session
user_code	String	One-time user verification code. This operation is required when authorizing a device in use.
verification_uri	String	URI of the validation page for authorizing a device using the one-time user verification code

Parameter	Type	Description
verification_uri_complete	String	Alternate URL that the client can use to automatically start the browser. This procedure skips the manual steps of the user accessing the validation page and entering the code.

Example Request

Requesting device authorization

```
POST https://{hostname}/v1/device/authorize

{
  "client_id" : "example_client_id",
  "client_secret" : "example_client_secret",
  "start_url" : "https://example-start.example.com/start/url"
}
```

Example Response

Status code: 200

Successful

```
{
  "device_code" : "1234567890123456789012345678901234567890123456789012345678901234",
  "expires_in" : 1684955360,
  "interval" : 10,
  "user_code" : "1234567890123456",
  "verification_uri" : "https://example-erification.example.com/erification/url",
  "verification_uri_complete" : "https://example-erification-complete.example.com/erification/url"
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.24 Authorization Management

4.24.1 Logging Out of a User

Function

This API is used to log a user out of the portal.

URI

POST /v1/logout

Request Parameters

Table 4-1096 Parameters in the request header

Parameter	Mandatory	Type	Description
access-token	Yes	String	Access token issued by the creating token API Maximum length: **4096**

Response Parameters

None

Example Request

This API is used to log out of a user.

```
POST https://{hostname}/v1/logout
```

Example Response

None

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.25 Account Management

4.25.1 Listing Accounts

Function

This API is used to list all accounts assigned to a user.

URI

GET /v1/assigned-accounts

Table 4-1097 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results on a page Minimum value: **1** Maximum value: **2000** Default value: **200**
marker	No	String	Pagination marker, which is used only for paging interfaces Minimum length: **4** Maximum length: **400**

Request Parameters

Table 4-1098 Parameters in the request header

Parameter	Mandatory	Type	Description
access-token	Yes	String	Access token issued by the creating token API Maximum length: **4096**

Response Parameters

Status code: 200

Table 4-1099 Parameters in the response body

Parameter	Type	Description
account_list	Array of objects	Listed accounts
page_info	Object	Pagination information

Table 4-1100 account_list

Parameter	Type	Description
account_id	String	Globally unique ID of the account assigned to a user
account_name	String	Name of the account assigned to a user

Parameter	Type	Description
email_address	String	Email address of the account assigned to a user Minimum length: **1** Maximum length: **254**

Table 4-1101 page_info

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**.
current_count	Integer	Number of records returned on this page

Example Request

Listing all accounts assigned to a user

```
GET https://{hostname}/v1/assigned-accounts
```

Example Response

Status code: 200

Successful

```
{
  "account_list" : [ {
    "account_id" : "5146d03d8aaaaaaaaaaaabbae60620a5",
    "account_name" : "example-account-name",
    "email_address" : "email@example.com"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.26 Agency Management

4.26.1 Listing Account Agencies

Function

This API is used to list all agencies or trust agencies assigned to a user for an account.

URI

GET /v1/assigned-agencies

Table 4-1102 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Maximum number of results on a page Minimum value: **1** Maximum value: **2000** Default value: **200**
marker	No	String	Pagination marker, which is used only for paging APIs Minimum length: **4** Maximum length: **400**
account_id	Yes	String	Globally unique ID of an account

Request Parameters

Table 4-1103 Parameters in the request header

Parameter	Mandatory	Type	Description
access-token	Yes	String	Access token issued by the creating token API Maximum length: **4096**

Response Parameters

Status code: 200

Table 4-1104 Parameters in the response body

Parameter	Type	Description
agency_list	Array of objects	Listed agencies or trust agencies
page_info	Object	Pagination information

Table 4-1105 agency_list

Parameter	Type	Description
account_id	String	Globally unique ID of the account assigned to a user
agency_name	String	Name of the agency or trust agency assigned to a user
permission_set_name	String	Name of a permission set
agency_urn	String	Uniform Resource Name (URN) of an agency or trust agency
description	String	Description

Table 4-1106 page_info

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**.
current_count	Integer	Number of records returned on this page

Example Request

Listing all agencies or trust agencies assigned to a user for an account

```
GET https://{hostname}/v1/assigned-agencies
```

Example Response

Status code: 200

Successful


```
{
  "agency_list" : [ {
    "account_id" : "5146d03d8aaaaaaaaaaabbae60620a5",
    "agency_name" : "example-agency-name",
    "permission_set_name" : "example-permission-set-name",
    "agency_urn" : "example-agency-urn",
    "description" : "example agency"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

4.27 Credentials Management

4.27.1 Obtaining Agency Credentials

Function

This API is used to obtain the STS short-term credentials for the agency or trust agency assigned to a user.

URI

GET /v1/credentials

Table 4-1107 Query parameters

Parameter	Mandatory	Type	Description
target_account_id	Yes	String	Globally unique ID of the target account.
agency_urn	Yes	String	Uniform Resource Name (URN) of an agency or trust agency.

Request Parameters

Table 4-1108 Parameters in the request header

Parameter	Mandatory	Type	Description
access-token	Yes	String	Access token issued by the creating token API. Maximum length: **4096**

Response Parameters

Status code: 200

Table 4-1109 Parameters in the response body

Parameter	Type	Description
agency_credentials	Object	Credential of an agency or trust agency assigned to a user.

Table 4-1110 agency_credentials

Parameter	Type	Description
access_key_id	String	ID of a temporary security credential.
expiration	Long	Expiration time of the temporary security credential.
secret_access_key	String	Secret key used to sign requests.
session_token	String	Temporary credential token.

Example Request

Obtaining the STS short-term credentials for the agency or trust agency assigned to a user

```
GET https://{hostname}/v1/credentials
```

Example Response

Status code: 200

Successful

```
{
  "agency_credentials" : {
    "access_key_id" : "example-access-key-id",
```



```
    "expiration" : 1684955360,
    "secret_access_key" : "example-secret-access-key",
    "session_token" : "string"
  }
}
```

Status Codes

For details, see **5.1 Status Codes**.

Error Codes

For details, see **Error Codes**.

5 Appendixes

5.1 Status Codes

Table 5-1 Status codes

Status Codes	Message	Description
100	Continue	The client continues sending the request. The server has received the initial part of the request and the client should continue sending the remaining part.
101	Switching Protocols	The requester has asked the server to switch protocols and the server has agreed to do so. The protocol can only be switched to a more advanced protocol. For example, the current HTTP protocol is switched to a later version.
201	Created	The request for creating a resource has been fulfilled.
202	Accepted	The request has been accepted, 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 does not return any content. The status code is returned in response to an HTTP OPTIONS request.
205	Reset Content	The server has fulfilled the request, but the requester is required to reset the content.

Status Codes	Message	Description
206	Partial Content	The server has fulfilled the partial GET request for the resource.
300	Multiple Choices	There are multiple options for the requested resource. The response contains a list of resource characteristics and addresses from which the user or user agent (such as a browser) can choose the most appropriate one.
301	Moved Permanently	The requested resource has been assigned a new permanent URI, and the new URI is contained in the response.
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. It 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 is invalid. The client should not repeat the request without modifications.
401	Unauthorized	The authorization information provided by the client is incorrect or invalid. Check the username and password.
402	Payment Required	This status code is reserved for future use.
403	Forbidden	The request is rejected. The server understands the request, but refuses to fulfill it. The client should not repeat the request without modifications.
404	NotFound	The requested resource cannot be found. The client should not repeat the request without modifications.

Status Codes	Message	Description
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. 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 cannot be found. 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 refuses to process a request because the request entity is too large. The server may disable the connection to prevent the client from sending requests consecutively. If the server cannot process the request temporarily, the response will contain a **Retry-After** field.
414	Request-URI Too Large	The request URI is too long for the server to process.
415	Unsupported Media Type	The server is unable to process the media format in the request.
416	Requested range not satisfiable	The requested range is invalid.

Status Codes	Message	Description
417	Expectation Failed	The server fails to meet the requirements of the **Expect** request header field.
422	UnprocessableEntity	The request is well-formed but is unable to be processed due to semantic errors.
429	TooManyRequests	The client sends excessive requests to the server within a given time (exceeding the limit on the access frequency of the client), or the server receives excessive requests within a given time (beyond its processing capability). 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 is able to receive the request but unable to understand the request.
501	Not Implemented	The server does not support the functionality required to fulfill the request.
502	Bad Gateway	The server was acting as a gateway or proxy and received an invalid response from the upstream server.
503	ServiceUnavailable	The requested service is invalid. The client should not repeat the request without modifications.
504	ServerTimeout	The request cannot be fulfilled within a given amount of time. This status code is returned to the client only when the **Timeout** parameter is specified in the request.
505	HTTP Version not supported	The server does not support the HTTP protocol version used in the request.

5.2 Error Codes

If an error code starting with **APIGW** is returned after you call an API, rectify the fault by referring to the instructions provided in **API Gateway Error Codes**.

Status Code	Error Code	Error Message	Description	Solution
400	IIC.4000	Bad Request: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
404	IIC.4000	Bad Request: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
404	IIC.4004	Not Found: {0}.	Resource not found.	Check whether the resource exists.
403	IIC.1000	No permission for action {0}.	Insufficient permissions.	Check whether you have required permissions.
403	IIC.1001	Access denied: {0}	The dependent API cannot be accessed.	Check whether you have required and dependent permissions.
404	IIC.1002	Bad Request: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
403	IIC.1003	Bad Request: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
403	IIC.1004	Bad Request: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
409	IIC.1006	Concurrency conflicts. Try again later.	Concurrency conflicts. Try again later.	Check whether the request parameters conflict and try again.
409	IIC.1007	Data modification failed.	Modification failed.	Check whether any data conflicts occur.
409	IIC.1204	The permission set already exists.	Permission set already created.	Check whether the permission set has already been created.
404	IIC.1205	The permission set does not exist.	Permission set not found.	Check whether the permission set exists.

Status Code	Error Code	Error Message	Description	Solution
409	IIC.1206	A permission set with the same name already exists.	Duplicate permission set name.	Check whether the permission set with the same name has already been created.
409	IIC.1207	Duplicate system-defined policy or identity policy.	Duplicate system-defined policy or identity policy.	Check whether the same system-defined policy or identity policy has been attached to the permission set.
500	IIC.1209	Bad Request: {0}.	Organizations operation error.	Contact technical support.
400	IIC.1210	Account not found.	Account not found.	Check whether the account exists and is managed in Organizations.
409	IIC.1210	The permission set has been attached to accounts and cannot be deleted.	The permission set has been attached to accounts and cannot be deleted.	Detach the permission set and try again.
404	IIC.1211	System-defined policy or identity policy not found.	System-defined policy or identity policy not found.	Check whether the system-defined policy or identity policy has been attached to the permission set.
404	IIC.1212	Request ID not found.	Request identified by the ID not found.	Check whether the request ID is correct.
400	IIC.1214	Region not registered in the service.	Region not registered.	Check whether the region has been registered.
403	IIC.1215	This operation is available only for the organization's administrator.	Only the Organizations administrator has permission to perform this operation.	Log in as the Organizations administrator and try again.

Status Code	Error Code	Error Message	Description	Solution
409	IIC.1216	Only one region can be registered.	Only one region can be registered.	Check whether another region has been registered.
404	IIC.1217	HTTP request header {0} not found.	HTTP request header not found.	Check whether the required HTTP request header is contained.
400	IIC.1218	Invalid X-Request-Proof request header.	Invalid request proof header.	Check whether the request proof header is correct.
400	IIC.1219	Failed to obtain the identity token.	Failed to obtain the temporary credential.	Check whether the request proof header used to obtain the temporary credential is correct.
403	IIC.1219	Failed to obtain the identity token.	Failed to obtain the temporary credential.	Check whether the request proof header used to obtain the temporary credential is valid.
400	IIC.1220	Failed to create service-linked agencies. Try again later.	Failed to create service-linked agencies. Try again later.	Check whether the request parameter is correct.
400	IIC.1221	Failed to enable trusted services. Try again later.	Failed to enable the trusted service. Failed to integrate IAM Identity Center with Organizations.	Check whether the request parameter is correct.
409	IIC.1222	IAM Identity Center has been enabled in another region.	Account ID already in use.	Check whether a service instance has been created for the account.
400	IIC.1223	Organizations not enabled.	Organizations not enabled.	Enable Organizations first.

Status Code	Error Code	Error Message	Description	Solution
404	IIC.1225	Failed to update the permission set status because the permission set is not attached to accounts.	Authentication failed because the permission set is not attached to the account.	Attach the permission set to the account.
400	IIC.1227	Identity source creation failed.	Failed to create the identity source.	Check whether the request parameter is correct.
500	IIC.1227	Identity source creation failed.	Failed to create the identity source.	Contact technical support.
400	IIC.1228	Identity source deletion failed.	Failed to delete the identity source.	Check whether the request parameter is correct.
500	IIC.1229	No service instance can be deleted.	Failed to delete the identity source.	Contact technical support.
400	IIC.1230	Service-linked agency deletion failed.	Failed to delete the service-linked agency.	Check whether the request parameter is correct.
400	IIC.1231	Failed to query the groups which the user belongs to.	Failed to query the groups where the user is added.	Check whether the request parameter is correct.
500	IIC.1231	Failed to query the groups which the user belongs to.	Failed to query the groups where the user is added.	Contact technical support.
400	IIC.1236	Invalid {0}	Invalid parameter.	Check whether the request parameter is valid.
403	IIC.1242	Please enable the service instance first.	Service instance not enabled.	Enable the service instance first.
400	IIC.1243	Failed to create the trust agency.	Failed to create the trust agency.	Check whether the request parameter is correct.
400	IIC.1244	Authentication failed.	Failed to check permissions.	Check whether the request parameter is correct.

Status Code	Error Code	Error Message	Description	Solution
403	IIC.1244	Authentication failed.	Failed to check permissions.	Check whether you have permission to perform this operation.
500	IIC.1244	Authentication failed.	Failed to check permissions.	Contact technical support.
400	IIC.1245	Only one instance can be provisioned.	Only one instance can be enabled.	Check whether the instance has been enabled.
400	IIC.1246	System-defined identity policy whose ID is {0} not found.	System-defined identity policy whose ID is {policyId} not found.	Check whether the ID of the system-defined identity policy is correct.
500	IIC.1247	Failed to delete the trust agency.	Failed to delete the trust agency.	Contact technical support.
500	IIC.1248	Failed to query the trust agency.	Failed to query the trust agency.	Contact technical support.
400	IIC.1249	Deletion failed. Associated account not found.	Associated account is not found and cannot be deleted.	Check whether the permission set is attached to the account.
400	IIC.1250	Associated principal is not found and cannot be deleted.	Associated principal is not found and cannot be deleted.	Check whether the permission set is attached to the principal.
400	IIC.1252	Incorrect format of the X-Request-Proof request header.	Failed to parse the HTTP authorization header.	Check whether the format of the HTTP authorization header is correct.
400	IIC.1253	Failed to deregister the region because an associated service instance exists.	The region cannot be deleted when the service instance exists.	Disable the service instance first.
404	IIC.1254	No region registered.	Registered region not found.	Check whether the region has been registered.
409	IIC.1257	Duplicate entity objects.	Duplicate entity objects.	Check whether the data already exists.

Status Code	Error Code	Error Message	Description	Solution
400	IIC.1258	The start time cannot be later than the end time.	The start time cannot be later than the end time.	Ensure that the start time is earlier than the end time.
404	IIC.1259	Service instance not found.	Instance not found.	Check whether the service instance is created.
500	IIC.1260	Internal server error.	Internal service error.	Contact technical support.
400	IIC.1261	Failed to obtain the identity source information.	Failed to query the connected identity source.	Check whether the identity source exists.
404	IIC.1000	No permission to attach the account.	You do not have permission to attach the account.	Check whether the account has been added to Organizations.
409	IIC.1000	This account does not have this service instance.	The service instance is not found in this account.	Check whether the account ID and instance ID are correct.
409	IIC.1261	Failed to permanently delete SDR meter database data fields.	Failed to permanently delete data fields from the SDR meter database.	Check whether the data already exists.
400	IIC.1263	The account has not applied for OBT.	You have not applied for an OBT.	Apply for an OBT first.
400	IIC.1264	Account tag query failed.	An error occurred in account tag query.	Check whether the request parameter is correct.
403	IIC.1265	HTTP request header not found.	HTTP request header not found.	Check whether the required HTTP request header is contained.
400	IIC.1266	HTTP request header not found.	Invalid HTTP request header.	Check whether the HTTP request header is valid.

Status Code	Error Code	Error Message	Description	Solution
400	IIC.1267	Synchronization failure: account:{0}, permissionSet:{1}, The detailed causes of the failure:{2}.	Failed to bind the authorization.	Check whether the request parameter is correct.
403	IIC.1269	Failed to request for assuming with service principal.	Failed to obtain the agency credential.	Check whether you have permission to perform this operation.
400	IIC.1270	Failed to obtain the MFA settings of the identity source.	Failed to obtain the MFA settings of the identity source.	Check whether the request parameter is correct.
409	IIC.1270	The alias can be modified only once.	Identity source ID alias has been created.	Check whether the identity source ID alias has been created.
400	IIC.1271	Failed to update the MFA settings of the identity source.	Failed to update the MFA settings of the identity source.	Check whether the request parameter is correct.
409	IIC.1271	The alias already exists.	Duplicate identity source ID alias.	Change the alias.
403	IIC.1272	No permission to perform this operation.	You do not have permission to enable or disable the service instance.	Check whether you have required permissions.
400	IIC.1273	The identity source does not belong to the account.	The identity source does not belong to the account.	Check whether the identity source belongs to the corresponding management account.
403	IIC.1273	The operation is not allowed because the account is frozen.	Account frozen. Operation not allowed.	Check whether the account is frozen.
403	IIC.1274	The operation is not allowed because the account is restricted.	Account restricted. Operation not allowed.	Check whether the account is restricted.

Status Code	Error Code	Error Message	Description	Solution
400	IIC.1275	The region is invalid or IAM Identity Center cannot be enabled in the region.	The region is invalid or IAM Identity Center cannot be enabled in this region.	Check whether the region is valid.
400	IIC.1276	Service instance not found.	Instance not found.	Check whether the request parameter is correct.
404	IIC.1276	Service instance not found.	Instance not found.	Check whether the instance exists.
400	IIC.1277	Agency creation failed.	Failed to create the agency.	Check whether the request parameter is correct.
500	IIC.1278	Agency deletion failed.	Failed to delete the agency.	Contact technical support.
500	IIC.1279	Role query failed.	Failed to query the policy.	Contact technical support.
500	IIC.1280	Agency query failed.	Failed to query the agency.	Contact technical support.
404	IIC.1281	Role ID {roleId} not found.	Role ID {roleId} not found.	Check whether the role ID exists.
409	IIC.1282	A conflict occurred during the service-linked agency creation. Try again later.	A conflict occurred during the service-linked agency creation. Try again later.	Check whether any conflicts occur during the service-linked agency creation and try again later.
400	IIC.1284	Failed to process Organizations broadcast messages.	An error occurred when IAM Identity Center consumes Organizations events.	Check whether the request parameter is correct.
403	IIC.1284	Failed to process Organizations broadcast messages.	An error occurred when IAM Identity Center consumes Organizations events.	Check whether permissions are sufficient.

Status Code	Error Code	Error Message	Description	Solution
500	IIC.1284	Failed to process Organizations broadcast messages.	An error occurred when IAM Identity Center consumes Organizations events.	Contact technical support.
400	IIC.1285	Custom role creation failed.	Failed to create the custom policy.	Check whether the custom policy is correct.
400	IIC.1286	Custom role update failed.	Failed to update the custom policy.	Check whether the custom policy is correct.
500	IIC.1287	Custom role deletion failed.	Failed to delete the custom policy.	Contact technical support.
500	IIC.1290	Authorization association not found.	Authorization association not found.	Contact technical support.
403	IIC.1291	The target account does not belong to the organization.	The target account does not belong to the organization.	Check whether the target account is in the organization.
400	IIC.1293	Size limit exceeded. A policy content can contain a maximum number of 6,144 characters.	The size of the policy content exceeds the upper limit.	Check whether the policy content is too large.
500	IIC.1300	Internal server error.	Internal service error.	Contact technical support.
409	IIC.1301	Failed to create another identity source because an identity source has been configured for the service instance.	The instance already has an identity source connected.	Check whether the instance has an identity source connected.
400	IIC.1302	Account not found.	No Organizations information found for the account.	Check whether the request parameter is correct.
400	IIC.1303	Organizations not enabled.	Organizations not enabled.	Enable Organizations first.
500	IIC.1304	Bad Request: {0}.	Organizations operation error.	Contact technical support.

Status Code	Error Code	Error Message	Description	Solution
403	IIC.1305	This operation is available only for the organization's administrator.	Only the Organizations administrator has permission to perform this operation.	Log in as the Organizations administrator and try again.
409	IIC.1306	The {0} is associated with an account. Disassociate the account and try again.	The principal is associated with an account. Disassociate the account and try again.	Disassociate the principal from the account and try again.
404	IIC.1307	Principal not found or principal type not correct.	Principal not found or principal type not correct.	Check whether the principal exists and whether the principal type is correct.
400	IIC.1308	Identity source not found.	Identity source not found.	Check whether the identity source ID is correct.
404	IIC.1308	Identity source not found.	Identity source not found.	Check whether the identity source exists.
500	IIC.1309	Failed to obtain the access token.	Failed to obtain the PKI token.	Contact technical support.
400	IIC.1310	Duplicate username or email address.	Duplicate username or email address.	Try another username or email address.
400	IIC.1311	The maximum number of allowed users has been reached.	The maximum number of users allowed in the identity source has been reached.	Check the user quota. If the quota does not meet your requirements, apply for a higher quota.
404	IIC.1312	User not found.	User not found.	Check whether the user exists.
404	IIC.1313	User extended attributes not found.	User extended attributes not found.	Check whether the user attributes are complete.

Status Code	Error Code	Error Message	Description	Solution
400	IIC.1314	Invalid password.	The password complexity does not meet requirements.	Use a more complex password.
400	IIC.1315	The password cannot be the same as the old password or one-time password.	The new password must be different from the old password and one-time password.	Enter another password.
404	IIC.1316	Unique user ID not found.	Unique user ID not found.	Check whether the request parameter is correct.
400	IIC.1317	User disabled.	Repeat disablement.	Check whether the object has already been disabled.
400	IIC.1318	User enabled.	Repeat enablement.	Check whether the object has already been enabled.
400	IIC.1319	Login credentials cannot be verified. Please try again.	Incorrect username or password.	Check whether the login credential is correct and try again.
404	IIC.1319	We could not verify your sign-in credentials. Please try again.	Username or password not found.	Check whether the username or password exists.
400	IIC.1320	User disabled.	User disabled.	Check whether the user is enabled.
400	IIC.1321	Duplicate email.	Duplicate email address.	Try another email address.
500	IIC.1322	Algorithm not found: {0}.	Algorithm not found.	Contact technical support.
400	IIC.1324	The new password must be different from the username.	The new password must be different from the username.	Enter another password.
400	IIC.1325	Invalid one-time password.	Invalid one-time password.	Check whether the one-time password is correct.

Status Code	Error Code	Error Message	Description	Solution
500	IIC.1326	Internal server error: {0}.	Internal service error.	Contact technical support.
400	IIC.1327	Invalid metadata.	Invalid SAML metadata.	Check whether the request parameter is correct.
400	IIC.1328	IdP configuration already exists.	IdP configuration already exists and cannot be created again.	Check whether the IdP configuration already exists.
400	IIC.1329	The IdP configuration status is incorrect.	The IdP configuration status is incorrect.	Check whether the IdP configuration status is correct.
404	IIC.1330	IdP configuration not found.	IdP configuration not found.	Check whether the IdP configuration exists.
400	IIC.1331	IdP tenant already exists.	IdP tenant already exists.	Check whether the IdP tenant already exists.
404	IIC.1332	Tenant ID not found.	IdP tenant not found.	Check whether the IdP tenant exists.
400	IIC.1333	Failed to delete the tenant because it is associated with a bearer token.	Failed to delete the provisioning tenant because it is associated with a token.	Delete the token first.
404	IIC.1334	Bearer token ID not found.	Token not found.	Check whether the token exists.
400	IIC.1335	The maximum number of allowed bearer tokens has been reached.	The maximum number of tokens has been reached.	Check the token quota.
400	IIC.1336	Username verification failed.	Incorrect username.	Check whether the request parameter is correct.
403	IIC.1337	No permission for action {0}.	No sufficient permissions.	Check whether you have permission to perform this operation.

Status Code	Error Code	Error Message	Description	Solution
403	IIC.1338	Request parameter is required.	The parameter value cannot be empty.	Check whether the parameter is correct.
403	IIC.1339	Service instance not found.	Parameter error. Service instance not found.	Check whether the parameter is correct.
409	IIC.1341	Duplicate display name of the group.	The display name of the group already exists.	Try another display name.
409	IIC.1342	Duplicate entity objects.	Failed to insert data into the database.	Check whether the data already exists.
404	IIC.1343	Group not found.	Group not found.	Check whether the group exists.
400	IIC.1344	The query condition must be an external ID or a unique attribute, and they cannot be specified at the same time.	Invalid alternative identifier.	Set the alternative identifier to **external_id** or **unique_attribute**.
400	IIC.1348	The query condition must be an external ID or a unique attribute, and they cannot be specified at the same time.	Either **external_id** or **unique_attribute** is required.	Check whether the alternative identifier uses only one condition.
404	IIC.1349	The attribute_path must be unique.	The path attribute must be unique.	Ensure that the path attribute is unique.
400	IIC.1351	The maximum number of allowed groups has been reached.	The maximum number of groups allowed in the identity source has been reached.	Check the group quota. If the quota does not meet your requirements, apply for a higher quota.
400	IIC.1352	The identity source does not belong to the account.	The identity source does not belong to the account.	Check whether the identity source belongs to the corresponding management account.

Status Code	Error Code	Error Message	Description	Solution
400	IIC.1353	The display name of the group is required.	The display name of the user group cannot be empty.	Check whether the display name of the user group is valid.
400	IIC.1370	The association between users and groups already exists.	The group membership already exists.	Check whether the user has been added to the group.
404	IIC.1371	The association between users and group does not exist.	Membership identified by the ID not found.	Check whether the membership association ID is correct.
400	IIC.1372	Group not found.	Group not found.	Check whether the group exists.
404	IIC.1372	Group not found.	Group not found.	Check whether the group exists.
400	IIC.1373	User not found.	User not found.	Check whether the user exists.
404	IIC.1373	User not found.	User not found.	Check whether the user exists.
404	IIC.1374	The association between users and group does not exist.	Group membership not found.	Check whether the user is added to the group.
404	IIC.1375	Group member not found.	Member not found.	Check whether all requested members exist.
400	IIC.1380	The start time cannot be later than the end time.	The start time must be earlier than the end time.	Ensure that the start time is earlier than the end time.
500	IIC.1381	Request processing failed due to an unknown error, exception, or fault on the internal server.	Request processing failed due to an unknown error, exception, or fault on the internal server.	Contact technical support.
409	IIC.1382	Failed to permanently delete database data fields.	Failed to permanently delete database data fields.	Check whether the data already exists.

Status Code	Error Code	Error Message	Description	Solution
400	IIC.1383	The account has not applied for OBT.	Beta account ID required.	Use a beta account.
400	IIC.1384	Account tag query failed.	An error occurred in account tag query.	Check whether the request parameter is correct.
404	IIC.1385	HTTP request header not found.	HTTP request header not found.	Check whether the required HTTP request header is contained.
400	IIC.1386	HTTP request header not found.	Invalid HTTP request header.	Check whether the HTTP request header is valid.
400	IIC.1387	MFA device {0} not found.	MFA device not found.	Check whether the parameter is correct.
400	IIC.1388	The maximum number of allowed MFA devices has been reached.	Failed to add MFA devices because the maximum number of MFA devices allowed for a user has been reached.	Check the MFA quota.
400	IIC.1389	Incorrect format of the X-Request-Proof request header.	Incorrect authentication header pattern.	Check whether the authentication header pattern is correct.
404	IIC.1390	HTTP request header {0} not found.	HTTP request header not found.	Check whether the HTTP request header exists.
400	IIC.1391	Invalid X-Request-Proof request header.	Incorrect request proof.	Check whether the request header parameter is correct.
400	IIC.1392	Failed to obtain the identity token.	Failed to obtain the STS credential.	Check whether the request parameter is correct.
403	IIC.1392	Failed to obtain the identity token.	Failed to obtain the STS credential.	Check whether you have sufficient permissions.

Status Code	Error Code	Error Message	Description	Solution
403	IIC.1393	The operation is not allowed because the account is frozen.	Account frozen. Operation not allowed.	Check whether the account is frozen.
403	IIC.1394	The operation is not allowed because the account is restricted.	Account restricted. Operation not allowed.	Check whether the account is restricted.
404	IIC.1398	Tenant not found.	Tenant not found.	Check whether the tenant exists.
400	IIC.1399	Failed to obtain the bearer token.	Failed to obtain the bearer token.	Check whether the parameter is correct.
400	IIC.1400	Bad Request: {0}.	Failed to create an access token.	Check whether the request parameter is correct.
500	IIC.1402	Bad Request: {0}.	Failed to create an access token.	Contact technical support.
400	IIC.1404	Access denied: {0}.	Access denied.	Check whether the request parameter is correct.
403	IIC.1404	Access denied: {0}.	Access denied.	Check whether you have permission to perform this operation.
400	IIC.1405	Bad Request: {0}.	Failed to verify the request parameter.	Check whether the request parameter is correct.
500	IIC.1405	Bad Request: {0}.	Failed to verify the request parameter.	Contact technical support.
404	IIC.1406	Application not found.	Application not found.	Check whether the application exists.
400	IIC.1407	Failed to request the authorization of the account.	Profile not found.	Check whether the request parameter is correct.
400	IIC.1409	Invalid token.	Invalid ID token.	Check whether the ID token is valid.
401	IIC.1410	{0}.	Unauthorized.	Perform authorization as prompted.

Status Code	Error Code	Error Message	Description	Solution
401	IIC.1410	Failed to verify the session because the token is not found.	Failed to verify the session because the token is not found.	Check whether the session has expired.
400	IIC.1411	Client registration error.	An exception occurred when you register the client.	Check whether the request parameter is correct.
500	IIC.1411	Client registration error.	An exception occurred when you register the client.	Contact technical support.
500	IIC.1412	Algorithm not found: {0}.	Algorithm not found.	Check whether the algorithm is correct or contact technical support.
400	IIC.1413	Invalid session state: {0}.	Invalid session state identifier.	Check whether the session status identifier is correct.
400	IIC.1414	Redis error.	Redis operation error.	Check whether the request parameter is correct.
400	IIC.1415	Failed to obtain the login token: {0}.	Failed to obtain the login token.	Check whether the request parameter is correct.
500	IIC.1415	Failed to obtain the login token: {0}.	Failed to obtain the login token.	Contact technical support.
500	IIC.1416	Internal server error: {0}.	Internal service error.	Contact technical support.
404	IIC.1417	Identity source ID not found.	Identity source ID not found.	Check whether the identity source ID exists.
400	IIC.1418	The workflow cannot be created.	Failed to create a workflow.	Check whether the parameter is correct.
400	IIC.1420	An error occurred when activating the device authorization code.	An error occurred when activating the device authorization code.	Check whether the request parameter is correct.

Status Code	Error Code	Error Message	Description	Solution
400	IIC.1420	An error occurred when canceling the device authorization code.	An error occurred when canceling the device authorization code.	Check whether the request parameter is correct.
403	IIC.1500	Invalid Token.	Invalid access token.	Check whether the access token is valid.
500	IIC.1501	Failed to obtain the identity token: {0}.	Failed to obtain the identity token.	Contact technical support.
500	IIC.1502	Failed to list accounts for the user: {0}.	Failed to obtain the account list.	Contact technical support.
500	IIC.1503	Failed to list agencies for the account: {0}.	Failed to list agencies or trust agencies for the account.	Contact technical support.
500	IIC.1504	Token verification failed: {0}.	Failed to verify the access token.	Contact technical support.
400	IIC.1505	Invalid parameter: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
500	IIC.1506	Algorithm not found.	Algorithm not found.	Check whether the algorithm is correct or contact technical support.
400	IIC.1507	Failed to obtain the service instance information: {0}.	Failed to obtain the service instance information.	Check whether the request parameter is correct.
500	IIC.1507	Failed to obtain the service instance information: {0}.	Failed to obtain the service instance information.	Contact technical support.
400	IIC.1508	Failed to delete the MFA device: {0}.	Failed to delete the MFA device for the user.	Check whether the parameter is correct.
500	IIC.1508	Failed to delete the MFA device: {0}.	Failed to delete the MFA device for the user.	Contact technical support.

Status Code	Error Code	Error Message	Description	Solution
400	IIC.1509	Failed to create the workflow: {0}.	Failed to create a workflow.	Check whether the parameter is correct.
500	IIC.1509	Failed to create the workflow: {0}.	Failed to create a workflow.	Contact technical support.
400	IIC.1511	Failed to obtain the MFA settings: {0}.	Failed to obtain the MFA management settings of the user.	Check whether the parameter is correct.
500	IIC.1511	Failed to obtain the MFA settings: {0}.	Failed to obtain the MFA management settings of the user.	Contact technical support.
400	IIC.1512	Failed to list MFA devices for the user: {0}.	Failed to list MFA devices for the user.	Check whether the parameter is correct.
500	IIC.1512	Failed to list MFA devices for the user: {0}.	Failed to list MFA devices for the user.	Contact technical support.
500	IIC.1513	Request processing failed due to an unknown error, exception, or fault on the internal server.	Request processing failed due to an unknown error, exception, or fault on the internal server.	Contact technical support.
400	IIC.1514	Failed to update the MFA device: {0}.	Failed to update MFA devices for the user.	Check whether the parameter is correct.
500	IIC.1514	Failed to update the MFA device: {0}.	Failed to update MFA devices for the user.	Contact technical support.
400	IIC.1515	Failed to obtain the permission set.	Failed to obtain the permission set.	Check whether the parameter is correct.
500	IIC.1515	Failed to obtain the permission set.	Failed to obtain the permission set.	Contact technical support.
400	IIC.1516	Email verification failed: {0}.	Email verification failed.	Check whether the parameter is correct.
500	IIC.1516	Email verification failed: {0}.	Email verification failed.	Contact technical support.

Status Code	Error Code	Error Message	Description	Solution
500	IIC.1517	Failed to get the PKI token.	Failed to obtain the PKI token.	Contact technical support.
403	IIC.1518	Read permission does not support MFA registration.	Read permissions do not support MFA binding.	Check whether permissions are sufficient.
403	IIC.1519	MFA disabled.	MFA disabled.	Enable MFA first.
400	IIC.1520	Invalid access token.	Invalid access token.	Check whether the access token is valid.
404	IIC.1600	Client not found.	Client not found.	Check whether the client ID is correct.
403	IIC.1601	Client expired.	The client has expired.	Check whether the client has expired. If yes, add the client again.
403	IIC.1602	Client secret expired.	The client secret key has expired.	Check whether the client secret key has expired. If yes, add the client again.
500	IIC.1603	Internal server error: {0}.	Internal service error.	Contact technical support.
401	IIC.1604	Invalid token.	Invalid access token.	Apply for a new access token and try again.
500	IIC.1605	Algorithm not found: {0}.	Algorithm not found.	Contact technical support.
400	IIC.1606	Invalid parameter: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
403	IIC.1606	Invalid parameter: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
404	IIC.1606	Invalid parameter: {0}.	Invalid request parameter.	Check whether the request parameter is correct.

Status Code	Error Code	Error Message	Description	Solution
400	IIC.1607	Failed to verify the JWT signature: {0}.	JWT token signature verification error.	Check whether the JWT token is correct.
400	IIC.1608	Authorization pending exception.	Authorization pending exception.	Try again later.
400	IIC.1609	The client does not support {0}.	Client not supported.	Check whether the request is correct.
500	IIC.1610	Internal server error.	Internal service error.	Contact technical support.
500	IIC.1611	Failed to obtain the access token.	Failed to obtain the access token.	Contact technical support.
401	IIC.1612	Invalid authorization type.	Invalid authorization type.	Check whether the authorization type is correct.
404	IIC.1613	Authorization rejected.	Authorization rejected.	Check whether the user agrees to the authorization.
400	IIC.1615	Requests of this type are not supported.	Request type not supported.	Check whether the request type is correct.
400	IIC.1616	The workflow is not supported.	Workflow not supported.	Check whether the workflow steps are correct.
400	IIC.1617	Failed to parse the ID token.	Failed to parse the ID token.	Check whether the ID token is valid.
400	IIC.1701	User verification exception.	User verification error.	Check whether the request parameter is correct.
500	IIC.1701	User verification exception.	User verification error.	Contact technical support.
400	IIC.1702	Login authentication error.	Login authentication error.	Check whether the authorization code is valid.
400	IIC.1703	Unsupported encoding.	Unsupported encoding.	Check whether the encoding of the request parameter is correct.

Status Code	Error Code	Error Message	Description	Solution
400	IIC.1704	Approval code error.	Authorization code approval error.	Check whether the authorization code is valid.
423	IIC.1705	User locked.	User locked or disabled.	Unlock or enable the user.
424	IIC.1706	User expired.	The user password has expired.	Change the user password.
400	IIC.1707	Incorrect username, password, or identity source ID.	Incorrect username, password, or identity source identifier.	Check whether the username, password, or identity source identifier is correct.
400	IIC.1708	An error occurred when obtaining the external IdP.	Failed to obtain the identity provider information.	Check whether the request parameter is correct.
400	IIC.1709	An error occurred when constructing the SAML request or response.	An error occurred when constructing the SAML request or response.	Check whether the request parameter is correct.
400	IIC.1710	No supported methods.	Unsupported method.	Check whether the request parameter is correct.
400	IIC.1711	An error occurred when obtaining SAML metadata.	Failed to obtain the SAML metadata.	Check whether the request parameter is correct.
400	IIC.1712	The signature certificate cannot be decoded.	Failed to verify the signature certificate.	Check whether the certificate signature is successful.
400	IIC.1714	Incorrect SAML response.	SAML response error.	Check whether the SAML response is correct.
500	IIC.1716	Algorithm not found: {0}.	Algorithm not found.	Contact technical support.
400	IIC.1717	Session expired.	Session expired.	Check whether the session is valid.
400	IIC.1718	Failed to reset the password.	Failed to reset the password.	Check whether the request parameter is valid.

Status Code	Error Code	Error Message	Description	Solution
400	IIC.1719	Username verification failed.	Username verification error.	Check whether the request parameter is correct.
400	IIC.1721	Session timed out or stopped working. Restart your workflow.	Session timed out or stopped working. Restart your workflow.	Restart your workflow.
400	IIC.1722	Request cannot be completed. Try again later.	Request cannot be completed. Try again later.	Try again later.
400	IIC.1724	Failed to process the workflow. Try again later.	Failed to process the workflow. Try again later.	Try again later.
400	IIC.1725	This operation cannot be performed.	This operation cannot be performed.	Check whether the request parameter is correct.
400	IIC.1726	Failed to verify the MFA code.	Failed to verify the MFA code.	Check whether the request parameter is valid.
400	IIC.1727	Failed to create an MFA device: {0}	Failed to create an MFA device.	Check whether the request parameter is correct.
400	IIC.1728	Failed to update the MFA device: {0}	Failed to update the MFA device.	Check whether the request parameter is correct.
400	IIC.1728	Failed to find the MFA device: {0}	Failed to find the MFA device.	Ensure that the device exists.
400	IIC.1729	Devices of this type cannot be registered again.	Devices of this type cannot be registered again.	Check whether the number of registered MFA devices has reached the upper limit.
400	IIC.1730	Failed to obtain the service instance information.	Failed to obtain the service instance information.	Check whether the request parameter is correct.
400	IIC.1731	Invalid session state.	Invalid session state.	Check whether the session has expired.

Status Code	Error Code	Error Message	Description	Solution
400	IIC.1734	User search failed.	Failed to retrieve users.	Check whether the request parameter is correct.
400	IIC.1735	Incorrect username, password, verification code, or identity source ID.	Incorrect username, password, verification code, or identity source ID.	Check whether the username, password, verification code, or identity source ID is correct.
400	IIC.1736	Workflow creation failed. Try again later.	Workflow creation failed. Try again later.	Try again later.
400	IIC.1737	Incorrect username, password, verification code, or identity source ID.	Incorrect username, password, verification code, or identity source ID.	Check whether the username, password, verification code, or identity source ID is correct.
500	IIC.1738	Failed to obtain the verification code.	Failed to obtain the verification code.	Contact technical support.
403	IIC.1739	Login failed. Contact the administrator to add an MFA device.	Login failed. Contact the administrator to add an MFA device.	Contact the administrator to add an MFA device.
400	IIC.1740	Invalid {0}	Invalid parameter.	Check whether the request parameter is valid.
400	IIC.1741	Invalid one-time password.	Invalid one-time password.	Check whether the one-time password is valid.
500	IIC.1750	Algorithm not found: {0}	Algorithm not found.	Contact technical support.
400	IIC.1751	Failed to update the email status: {0}	Failed to update the email status.	Check whether the request parameter is correct.

Table 5-2 SCIM error codes

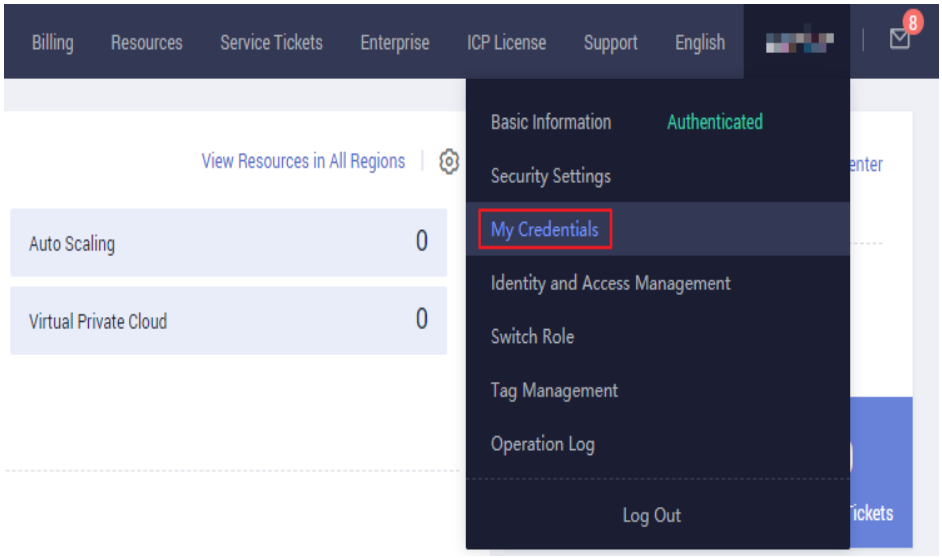
HTTP Status Code	Response Status Code	Error Message	Description	Solution
400	400	Bad Request: {0}	Unsupported encoding.	Check whether the encoding of the request parameter is correct.
404	404	User [{0}] not found.	User not found.	Check whether the user exists.
404	404	Group [{0}] not found.	Group not found.	Check whether the group exists.
404	404	Group member not found.	Member not found.	Check whether the user exists and is added to the group.
409	409	User [{0}] or email address already exists.	User already exists.	Check whether the user already exists.
409	409	Group [{0}] already exists.	Group already exists.	Check whether the group already exists.
500	500	There was an internal server error.	Internal service error.	Contact technical support.

5.3 Obtaining Information About Account, IAM User, Group, Project, Region, and Agency

Obtaining Account, IAM User, and Project Information

- **Using the console**
  a. On the Huawei Cloud homepage, click **Console** in the upper right corner.
  b. Hover over the username in the upper right corner and choose **My Credentials**.

Figure 5-1 My Credentials



c. View the account name, account ID, username, user ID, project name, and project ID on the **API Credentials** page.

The project ID varies depending on the region where the service is located.

Figure 5-2 Viewing the account, user, and project information

- **Calling an API**
  - For details about how to obtain a user ID, see **Listing IAM Users**.
  - For details about how to obtain a project ID, see **Querying Project Information**.

Obtaining User Group Information

Step 1 Log in to the IAM console, and choose **User Groups** in the navigation pane.

Step 2 Expand the details page of a user group and view the group name and ID.

----End

Obtaining Region Information

Step 1 Log in to the IAM console, and choose **Projects** in the navigation pane.

Step 2 The value in the **Project Name** column is the ID of the region which the project belongs to.

----End

Obtaining Agency Information

Step 1 Log in to the IAM console, and choose **Agencies** in the navigation pane.

Step 2 Hover over the desired agency. The name and ID of this agency are displayed in a dark pop-up box.

----End

5.4 Configuring SDK Client Authentication

The credential parameters vary depending on the initialization of different clients. You can refer to the following sample code to upload the appropriate credential.

```
// Initialize the IdentityCenterClient client.
IdentityCenterClient client = IdentityCenterClient.newBuilder()
    .withCredential(new GlobalCredentials()
        .withAk(ak)
        .withSk(sk))
    .build();
```

```
// Initialize the IdentityCenterStoreClient client.
IdentityCenterStoreClient client = IdentityCenterStoreClient.newBuilder()
    .withCredential(new BasicCredentials()
        .withAk(ak)
        .withSk(sk))
    .build();
```

```
// Initialize the IdentityCenterOIDCClient client.
IdentityCenterOIDCClient client = IdentityCenterOIDCClient.newBuilder()
    .withCredential(new IdentityCenterOIDCCredentials())
    .build();
```

```
// Initialize the IdentityCenterSCIMClient client.
IdentityCenterSCIMClient client = IdentityCenterSCIMClient.newBuilder()
    .withCredential(new IdentityCenterSCIMCredentials())
    .build();
```

```
// Initialize the IdentityCenterPortalAPIClient client.
IdentityCenterPortalAPIClient client = IdentityCenterPortalAPIClient.newBuilder()
    .withCredential(new IdentityCenterPortalAPICredentials())
    .build();
```

