

IAM Identity Center

API Reference

Issue 01
Date 2023-08-30



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks 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 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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 Before You Start	1
1.1 Description	1
1.2 API Calling	1
1.3 Endpoint	1
1.4 Constraints	1
1.5 Concepts	2
2 API Overview	4
3 Calling APIs	6
3.1 Making an API Request	6
3.2 Authentication	8
3.3 Response	8
4 API	11
4.1 Instance Management	11
4.1.1 Listing Instances	11
4.2 Access Control Attribute Management	14
4.2.1 Enabling Access Control Attributes for a Specified Instance	14
4.2.2 Obtaining Access Control Attributes for a Specified Instance	17
4.2.3 Updating Access Control Attributes for a Specified Instance	20
4.2.4 Disabling Access Control Attributes for a Specified Instance	23
4.3 Permission Set Management	24
4.3.1 Adding a System-defined Identity Policy	24
4.3.2 Deleting a Permission Set	26
4.3.3 Querying Permission Set Details	28
4.3.4 Updating a Permission Set	31
4.3.5 Deleting a System-defined Identity Policy	34
4.3.6 Querying Details About a Custom Identity Policy	36
4.3.7 Adding a Custom Identity Policy	38
4.3.8 Deleting a Custom Identity Policy	40
4.3.9 Listing Accounts Associated with a Permission Set	42
4.3.10 Listing System-defined Identity Policies	44
4.3.11 Listing Pre-provisioning Statuses of Permission Sets	47
4.3.12 Listing Permission Sets	51

4.3.13 Creating a Permission Set.....	54
4.3.14 Listing Permission Sets Provisioned to an Account.....	58
4.3.15 Pre-provisioning a Permission Set.....	61
4.3.16 Querying Pre-attachment Status Details of a Permission Set.....	64
4.3.17 Adding a System-defined Policy.....	67
4.3.18 Deleting a System-defined Policy.....	69
4.3.19 Listing System-defined Policies.....	71
4.4 Account Assignment Management.....	74
4.4.1 Removing Account Assignments.....	74
4.4.2 Querying Details about the Account Assignment Creation Status.....	78
4.4.3 Listing Account Assignment Creation Statuses.....	81
4.4.4 Listing Account Assignment Deletion Statuses.....	84
4.4.5 Listing Users or Groups Associated with an Account and a Permission Set.....	88
4.4.6 Creating Account Assignments.....	91
4.4.7 Querying Details about the Account Assignment Deletion Status.....	95
4.5 Tag Management.....	98
4.5.1 Listing Tags for the Specified Resource.....	98
4.5.2 Adding Tags to the Specified Resource.....	101
4.5.3 Removing the Specified Tag from the Specified Resource.....	104
4.6 User Management.....	106
4.6.1 Creating a User.....	106
4.6.2 Listing Users.....	113
4.6.3 Deleting a User.....	121
4.6.4 Querying User Details.....	124
4.6.5 Updating a User.....	131
4.6.6 Querying a User ID.....	134
4.7 Group Management.....	138
4.7.1 Creating a Group.....	138
4.7.2 Listing Groups.....	141
4.7.3 Deleting a Group.....	145
4.7.4 Updating a Group.....	147
4.7.5 Querying Group Details.....	149
4.7.6 Querying a Group ID.....	151
4.8 Group Membership Management.....	155
4.8.1 Adding a User to a Group.....	155
4.8.2 Listing Users in a Group.....	158
4.8.3 Listing Groups to which a User is Added.....	161
4.8.4 Removing a User from a Group.....	164
4.8.5 Querying the Group Membership.....	166
4.8.6 Querying the Group Membership ID.....	169
4.8.7 Querying Whether a User Is a Member of a Group.....	172
4.9 SCIM User Management.....	175

4.9.1 Creating a User.....	176
4.9.2 Listing Users.....	186
4.9.3 Querying User Details.....	193
4.9.4 Deleting a User.....	200
4.9.5 Updating a User.....	203
4.9.6 Partially Updating a User.....	213
4.10 SCIM Group Management.....	221
4.10.1 Creating a Group.....	221
4.10.2 Listing Groups.....	225
4.10.3 Querying Group Details.....	229
4.10.4 Deleting a Group.....	233
4.10.5 Partially Updating a Group.....	236
4.11 Service Provider (SP) Management.....	239
4.11.1 Querying the SP Configuration.....	239
4.12 Client Management.....	245
4.12.1 Registering a Client.....	245
4.13 Token Management.....	247
4.13.1 Creating a Token.....	247
4.14 Device Authorization Management.....	250
4.14.1 Requesting Device Authorization.....	250
4.15 Authorization Management.....	251
4.15.1 Logging Out of a User.....	252
4.16 Account Management.....	252
4.16.1 Listing Accounts.....	252
4.17 Agency Management.....	255
4.17.1 Listing Account Agencies.....	255
4.18 Credentials Management.....	257
4.18.1 Obtaining Agency Credentials.....	257
5 Appendixes.....	260
5.1 Status Codes.....	260
5.2 Error Codes.....	263
5.3 Obtaining Information About Account, IAM User, Group, Project, Region, and Agency.....	294
6 Change History.....	296

1 Before You Start

1.1 Description

IAM Identity Center helps you centrally manage your workforce identities and their access to multiple Huawei Cloud accounts. 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.

Before calling IAM Identity Center through an API, ensure that you are familiar with IAM concepts. For details, see [What Is IAM Identity Center?](#).

1.2 API Calling

IAM Identity Center supports Representational State Transfer (REST) APIs, allowing you to call APIs using HTTPS. For details about API calling, see [Calling APIs](#).

1.3 Endpoint

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](#).

1.4 Constraints

- For details about the quota limits of IAM Identity Center, see [Notes and Constraints](#).
- For more constraints, see API description.

1.5 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**

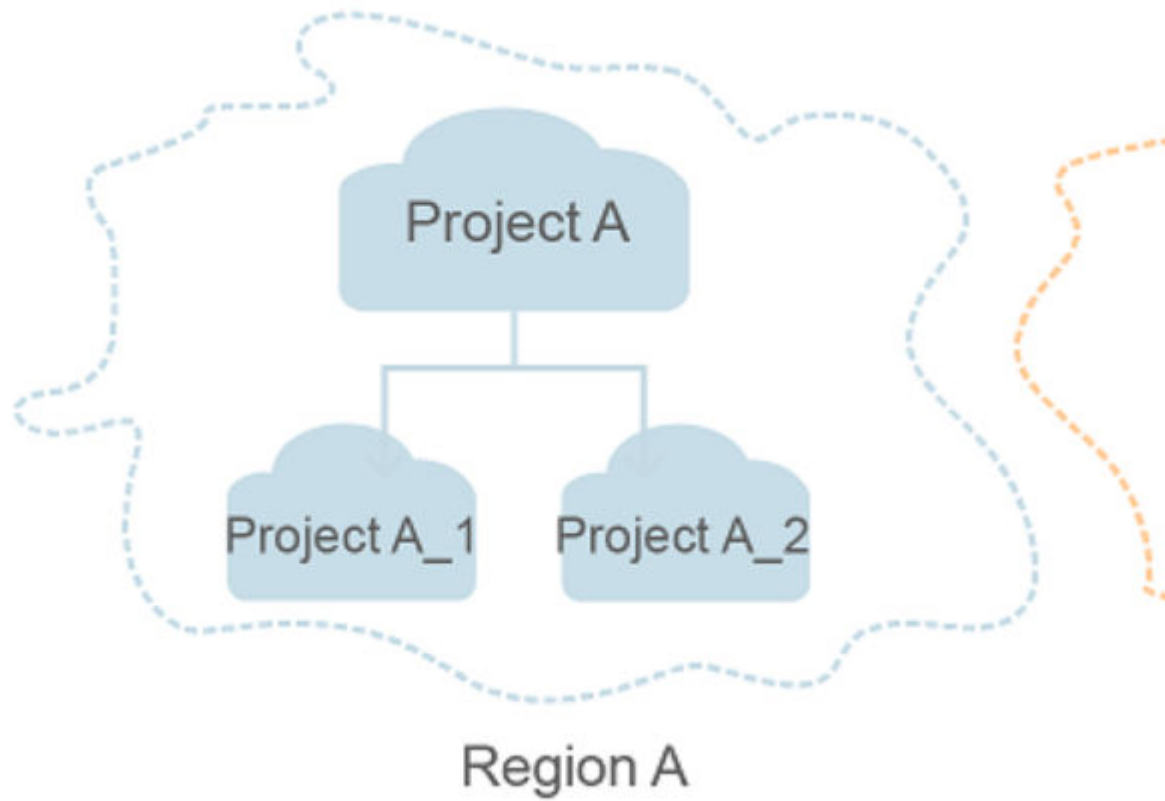
Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. 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 create 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
Instance Management	List instances.
Access Control Attribute Management	Enable, obtain, update, and disable access control attributes for a specified instance.
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.
Account Assignment Management	Add, delete, and query account assignments; query creation and deletion statuses of account assignments.
Tag Management	List, add, and remove tags for a specified permission set.
User Management	Add, delete, modify, and query users; query user IDs.
Group Management	Add, delete, modify, and query groups; query group IDs.
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.
SCIM User Management	Add, modify, and delete users based on the SCIM protocol.
SCIM Group Management	Add, modify, and delete groups based on the SCIM protocol.

Type	Description
Service Provider (SP) Management	Query the SCIM configuration in the service provider (SP).
Client Management	Register a client.
Token Management	Create a token.
Device Authorization Management	Request device authorization.
Authorization Management	Log out of a user.
Account Management	List account information.
Agency Management	List account agencies or trust agencies.
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 <i>Parameter name=Parameter value</i> . 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 [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 [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=xxxxxxxxxxxxxxxxxxxxx, SignedHeaders=content-type;host;x-sdk-date, Signature=xxxxxxxxxxxxxxxxxxxxx
```

(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 Code

A status code is a group of digits, ranging from 1xx to 5xx. It indicates the status of a request. For more information, see [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 [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 query the instance list of IAM Identity Center.

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

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

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-bd8baaaaaade60"
}],
"page_info" : {
  "next_marker" : null,
  "current_count" : 1
}
}
```

Status Codes

For details, see [Status Codes](#).

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.

URI

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

Table 4-8 Path parameters

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

Request Parameters

Table 4-9 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 4-10 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 4-11 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 4-12 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 4-13 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 4-14 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 4-15 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 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 Code

For details, see [Status Codes](#).

Error Code

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.

URI

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

Table 4-16 Path parameters

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

Request Parameters

Table 4-17 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 4-18 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
status	String	ABAC attribute configuration status Enumerated value: <ul style="list-style-type: none">• ENABLED• CREATION_IN_PROGRESS• CREATION_FAILED
status_reason	String	Details about the state of the specified attribute

Table 4-19 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 4-20 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 4-21 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 4-22** 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 4-23** 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

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 Code

For details, see [Status Codes](#).

Error Code

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.

URI

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

Table 4-24 Path parameters

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

Request Parameters

Table 4-25 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 4-26 Parameters in the request body

Parameter	Mandatory	Type	Description
instance_access_control_attribute_configuration	Yes	Object	Updates the attributes of the ABAC configuration

Table 4-27 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 4-28 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 4-29 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 4-30 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

Status code: 403**Table 4-31** 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 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 Code

For details, see [Status Codes](#).

Error Code

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.

URI

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

Table 4-32 Path parameters

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

Request Parameters

Table 4-33 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 4-34 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

Status code: 403

Table 4-35 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 access control attributes for a specified instance

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

Example Response

None

Status Code

For details, see [Status Codes](#).

Error Code

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.

URI

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

Table 4-36 Path parameters

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

Parameter	Mandatory	Type	Description
permission_set_id	Yes	String	Globally unique ID of a permission set

Request Parameters

Table 4-37 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 4-38 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 4-39 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 4-40 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 4-41** 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

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 [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.

URI

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

Table 4-42 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 4-43 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 4-44 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

Status code: 403

Table 4-45 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: 404

Table 4-46 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 a permission set according to the specified permission set ID

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

Example Response

None

Status Codes

For details, see [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.

URI

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

Table 4-47 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 4-48 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 4-49 Parameters in the response body

Parameter	Type	Description
permission_set	Object	Permission set details

Table 4-50 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

Parameter	Type	Description
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
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 4-51** 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 4-52** 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: 404

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

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 [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.

URI

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

Table 4-54 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 4-55 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 4-56 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 4-57 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 4-58** 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: 404**Table 4-59** 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 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 [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.

URI

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

Table 4-60 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 4-61 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 4-62 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 4-63 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 4-64 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: 404

Table 4-65 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 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 [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.

URI

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

Table 4-66 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 4-67 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 4-68 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 4-69** 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

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

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 Code

For details, see [Status Codes](#).

Error Code

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.

URI

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

Table 4-71 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 4-72 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
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 4-74 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 4-75 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 4-76 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

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 Code

For details, see [Status Codes](#).

Error Code

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.

URI

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

Table 4-77 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 4-78 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 4-79 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 4-80 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 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 Code

For details, see [Status Codes](#).

Error Code

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.

URI

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

Table 4-81 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 4-82 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
provisioning_status	No	String	Provisioning status of a permission set Enumerated value: <ul style="list-style-type: none">• LATEST_PERMISSION_SET_PROVISIONED• LATEST_PERMISSION_SET_NOT_PROVISIONED

Request Parameters

Table 4-83 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 4-84 Parameters in the response body

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

Table 4-85 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 4-86 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 4-87 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

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 [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.

URI

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

Table 4-88 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 4-89 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 4-90 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: 200

Table 4-91 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 4-92 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 4-93 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 4-94** 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 4-95 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 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 [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.

URI

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

Table 4-96 Path parameters

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

Table 4-97 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: <ul style="list-style-type: none">• IN_PROGRESS• SUCCEEDED• FAILED

Request Parameters

Table 4-98 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 4-99 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 4-100 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: <ul style="list-style-type: none">• IN_PROGRESS• FAILED• SUCCEEDED

Table 4-101 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 4-102 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 4-103** 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 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 [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.

URI

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

Table 4-104 Path parameters

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

Table 4-105 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 4-106 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 4-107** Parameters in the response body

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

Table 4-108 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 4-109 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 4-110** 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

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

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 [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.

URI

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

Table 4-112 Path parameters

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

Request Parameters

Table 4-113 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 4-114 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
tags	No	Array of objects	Tags to be attached to a permission set Array length: 0 - 50

Table 4-115 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 4-116 Parameters in the response body

Parameter	Type	Description
permission_set	Object	Permission set details

Table 4-117 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 4-118** 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 4-119** 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 4-120** 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 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 [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.

URI

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

Table 4-121 Path parameters

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

Table 4-122 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: <ul style="list-style-type: none">• LATEST_PERMISSION_SET_PROVISIONED• LATEST_PERMISSION_SET_NOT_PROVISIONED

Request Parameters

Table 4-123 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 4-124 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 4-125 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 4-126** 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

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

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 [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.

URI

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

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

Request Parameters

Table 4-129 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 4-130 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: <ul style="list-style-type: none">• ACCOUNT• ALL_PROVISIONED_ACCOUNTS

Response Parameters

Status code: 200

Table 4-131 Parameters in the response body

Parameter	Type	Description
permission_set_provisioning_status	Object	Authorization details of a permission set

Table 4-132 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

Parameter	Type	Description
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: <ul style="list-style-type: none">• IN_PROGRESS• FAILED• SUCCEEDED

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

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

Status code: 404**Table 4-135** 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

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" : "5146d03d8aaaaaaaaaaaaabbae60620a5",
  "target_type" : "ACCOUNT"
}
```

Example Response

Status code: 200

Successful

```
{
  "permission_set_provisioning_status" : {
    "account_id" : "5146d03d8aaaaaaaaaaaaabbae60620a5",
    "created_date" : "1677175760379",
    "failure_reason" : "",
    "permission_set_id" : "ps-8603aaaaaaaa14bd",
    "request_id" : "a1177591c8c7c49238e60563d34cad92",
    "status" : "SUCCEEDED"
  }
}
```

Status Codes

For details, see [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.

URI

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

Table 4-136 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 4-137 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
permission_set_provisioning_status	Object	Authorization details of a permission set

Table 4-139 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

Parameter	Type	Description
request_id	String	Unique ID of a request Minimum length: 36 Maximum length: 36
status	String	Authorization status of a permission set Enumerated value: <ul style="list-style-type: none">• IN_PROGRESS• FAILED• SUCCEEDED

Status code: 400**Table 4-140** 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 4-141** 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

Status code: 404**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

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": "5146d03d8aaaaaaaaaabbbae60620a5",
    "created_date": "1677175760379",
    "failure_reason": "",
    "permission_set_id": "ps-8603aaaaaaaa14bd",
    "request_id": "a1177591c8c7c49238e60563d34cad92",
    "status": "SUCCEEDED"
  }
}
```

Status Codes

For details, see [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.

URI

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

Table 4-143 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 4-144 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 4-145 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 4-146 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 4-147 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: 409

Table 4-148 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

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" : "ba5146848aaaaaaaaaaaa03de60620a5",
  "managed_role_name" : "role_example_456"
}
```

Example Response

None

Status Codes

For details, see [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.

URI

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

Table 4-149 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 4-150 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 4-151 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 4-152 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 4-153 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: 404**Table 4-154** 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 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" : "ba5146848aaaaaaaaaaaa03de60620a5"
}
```

Example Response

None

Status Codes

For details, see [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.

URI

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

Table 4-155 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 4-156 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 4-157 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 4-158 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 4-159 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 4-160 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 4-161** 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 4-162** 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 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": "ba5146848aaaaaaaaaaaa03de60620a5",
    "role_name": "role_example_456"
  } ],
  "page_info": {
    "next_marker": null,
    "current_count": 1
  }
}
```

Status Codes

For details, see [Status Codes](#).

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.

URI

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

Table 4-163 Path parameters

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

Request Parameters

Table 4-164 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 4-165 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: <ul style="list-style-type: none">• USER• GROUP
target_id	Yes	String	ID of the target account
target_type	Yes	String	Target type Enumerated value: <ul style="list-style-type: none">• ACCOUNT

Response Parameters

Status code: 200

Table 4-166 Parameters in the response body

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

Table 4-167 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: <ul style="list-style-type: none">• USER• GROUP
request_id	String	Unique ID of a request
status	String	Authorization status of a permission set Enumerated value: <ul style="list-style-type: none">• IN_PROGRESS• FAILED• SUCCEEDED
target_id	String	Unique ID of a target principal
target_type	String	Principal type Enumerated value: <ul style="list-style-type: none">• ACCOUNT

Status code: 400

Table 4-168 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 4-169** 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: 404**Table 4-170** 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 4-171** 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

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" : "5146d03d8aaaaaaaaaaaaabbae60620a5",
  "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 [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.

URI

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

Table 4-172 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 4-173 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 4-174 Parameters in the response body

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

Table 4-175 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

Parameter	Type	Description
principal_type	String	Principal type of an operation Enumerated value: <ul style="list-style-type: none">• USER• GROUP
request_id	String	Unique ID of a request
status	String	Authorization status of a permission set Enumerated value: <ul style="list-style-type: none">• IN_PROGRESS• FAILED• SUCCEEDED
target_id	String	Unique ID of a target principal
target_type	String	Principal type Enumerated value: <ul style="list-style-type: none">• ACCOUNT

Status code: 400**Table 4-176** 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 4-177** 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: 404

Table 4-178 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 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": "5146d03d8aaaaaaaaabbae60620a5",
    "target_type": "ACCOUNT"
  }
}
```

Status Codes

For details, see [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.

URI

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

Table 4-179 Path parameters

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

Table 4-180 Query parameters

Parameter	Mandatory	Type	Description
status	No	String	Status of the listing account assignment creation process Enumerated value: <ul style="list-style-type: none">• 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 4-181 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 4-182 Parameters in the response body

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

Table 4-183 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: <ul style="list-style-type: none">• IN_PROGRESS• FAILED• SUCCEEDED

Table 4-184 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 4-185** 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 4-186 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 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 [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.

URI

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

Table 4-187 Path parameters

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

Table 4-188 Query parameters

Parameter	Mandatory	Type	Description
status	No	String	Status of the listing account assignment deletion process Enumerated value: <ul style="list-style-type: none">• 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 4-189 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 4-190 Parameters in the response body

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

Table 4-191 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: <ul style="list-style-type: none">• IN_PROGRESS• FAILED• SUCCEEDED

Table 4-192 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 4-193 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

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

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" : "9238e6aaaaaaaaaaaaaaaaaaaa4cad92",
    "status" : "IN_PROGRESS"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

For details, see [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.

URI

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

Table 4-195 Path parameters

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

Table 4-196 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 4-197 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

Response Parameters

Status code: 200

Table 4-198 Parameters in the response body

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

Table 4-199 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: <ul style="list-style-type: none">• USER• GROUP

Table 4-200 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 4-201** 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

Status code: 403**Table 4-202** 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 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": "5146d03d8aaaaaaaaaaaaabbae60620a5",
    "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 [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.

URI

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

Table 4-203 Path parameters

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

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

Table 4-205 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• ACCOUNT

Response Parameters

Status code: 200

Table 4-206 Parameters in the response body

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

Table 4-207 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

Parameter	Type	Description
principal_type	String	Principal type of an operation Enumerated value: <ul style="list-style-type: none">• USER• GROUP
request_id	String	Unique ID of a request
status	String	Authorization status of a permission set Enumerated value: <ul style="list-style-type: none">• IN_PROGRESS• FAILED• SUCCEEDED
target_id	String	Unique ID of a target principal
target_type	String	Principal type Enumerated value: <ul style="list-style-type: none">• ACCOUNT

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

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

Status code: 404

Table 4-210 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 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" : "5146d03d8aaaaaaaaaaaaabbae60620a5",
  "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 [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.

URI

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

Table 4-211 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 4-212 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 4-213 Parameters in the response body

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

Table 4-214 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: <ul style="list-style-type: none">• USER• GROUP
request_id	String	Unique ID of a request
status	String	Authorization status of a permission set Enumerated value: <ul style="list-style-type: none">• IN_PROGRESS• FAILED• SUCCEEDED
target_id	String	Unique ID of a target principal
target_type	String	Principal type Enumerated value: <ul style="list-style-type: none">• ACCOUNT

Status code: 400**Table 4-215** 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 4-216 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: 404**Table 4-217** 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 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": "5146d03d8aaaaaaaaaaaaabbae60620a5",
    "target_type": "ACCOUNT"
  }
}
```

Status Codes

For details, see [Status Codes](#).

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.

URI

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

Table 4-218 Path parameters

Parameter	Mandatory	Type	Description
resource_type	Yes	String	Resource type Enumerated value: <ul style="list-style-type: none">• identitycenter:permissions et (permission set)
resource_id	Yes	String	Unique ID of a permission set Maximum length: 130

Table 4-219 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 4-220 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 4-221 Parameters in the response body

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

Table 4-222 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 4-223 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.

Status code: 400**Table 4-224** 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 4-225** 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 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 Code

For details, see [Status Codes](#).

Error Code

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.

URI

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

Table 4-226 Path parameters

Parameter	Mandatory	Type	Description
resource_type	Yes	String	Resource type Enumerated value: <ul style="list-style-type: none">identitycenter:permissions et (permission set)
resource_id	Yes	String	Unique ID of a permission set Maximum length: 130

Request Parameters

Table 4-227 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 4-228 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 4-229 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: 400

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

Status code: 403**Table 4-231** 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 4-232** 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

Adding tags to the specified resource

```
POST https://{hostname}/v1/instances/{resource_type}/{resource_id}/tags/create
{
  "tags": [ {
    "key": "keysting",
    "value": "valuestring"
  } ]
}
```

Example Response

None

Status Code

For details, see [Status Codes](#).

Error Code

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.

URI

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

Table 4-233 Path parameters

Parameter	Mandatory	Type	Description
resource_type	Yes	String	Resource type Enumerated value: <ul style="list-style-type: none">• identitycenter:permissions et (permission set)
resource_id	Yes	String	Unique ID of a permission set Maximum length: 130

Request Parameters

Table 4-234 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 4-235 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 4-236 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

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

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

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 Code

For details, see [Status Codes](#).

Error Code

For details, see [Error Codes](#).

4.6 User Management

4.6.1 Creating a User

Function

This API is used to create an IAM Identity Center user in the specified identity source.

URI

POST /v1/identity-stores/{identity_store_id}/users

Table 4-239 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source Minimum length: 12 Maximum length: 12

Request Parameters

Table 4-240 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 4-241 Parameters in the request body

Parameter	Mandatory	Type	Description
addresses	No	Array of objects	Address list of a user Array length: 1-1
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	Name of a user
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

Parameter	Mandatory	Type	Description
user_type	No	String	User type Minimum length: 1 Maximum length: 1024
password_mode	Yes	String	Password initialization mode, which can be one-time password or email address Enumerated value: <ul style="list-style-type: none">• OTP• EMAIL
enterprise	No	Object	Object that contains the user's work-related information

Table 4-242 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

Parameter	Mandatory	Type	Description
type	No	String	Address type Minimum length: 1 Maximum length: 1024

Table 4-243 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: <ul style="list-style-type: none">• NOT_VERIFIED• VERIFIED

Table 4-244 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

Parameter	Mandatory	Type	Description
honorific_prefix	No	String	Prefix of a user name Minimum length: 1 Maximum length: 1024
honorific_suffix	No	String	Suffix of a user name Minimum length: 1 Maximum length: 1024
middle_name	No	String	Middle name of a user Minimum length: 1 Maximum length: 1024

Table 4-245 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 4-246 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

Parameter	Mandatory	Type	Description
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 4-247 manager

Parameter	Mandatory	Type	Description
value	No	String	Manager Minimum length: 1 Maximum length: 1024

Response Parameters

Status code: 201

Table 4-248 Parameters in the response body

Parameter	Type	Description
identity_store_id	String	Globally unique ID of the 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 4-249 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403**Table 4-250** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 409**Table 4-251** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.6.2 Listing Users

Function

This API is used to list the IAM Identity Center users in the specified identity source.

URI

GET /v1/identity-stores/{identity_store_id}/users

Table 4-252 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source Minimum length: 12 Maximum length: 12

Table 4-253 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 4-254 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 4-255 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 4-256 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 4-257 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 the 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	Name of a user
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

Parameter	Type	Description
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
enabled	Boolean	Whether a user is enabled
enterprise	Object	Object that contains the user's work-related information

Table 4-258 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 4-259 users.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

Parameter	Type	Description
verification_status	String	String Verification status of an email address Enumerated value: <ul style="list-style-type: none">• NOT_VERIFIED• VERIFIED

Table 4-260 users.external_ids

Parameter	Type	Description
id	String	ID issued by an external identity provider Minimum length: 1 Maximum length: 256
issuer	String	Issuer of the external ID Minimum length: 1 Maximum length: 100

Table 4-261 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
honorific_prefix	String	Prefix of a user name Minimum length: 1 Maximum length: 1024
honorific_suffix	String	Suffix of a user name Minimum length: 1 Maximum length: 1024

Parameter	Type	Description
middle_name	String	Middle name of a user Minimum length: 1 Maximum length: 1024

Table 4-262 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 4-263 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 4-264 manager

Parameter	Type	Description
value	String	Manager Minimum length: 1 Maximum length: 1024

Status code: 400**Table 4-265** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403**Table 4-266** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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" : "5146d03d8aaaaaaaaaaaaabbae60620a5",
  "updated_at" : 1687184129926,
  "updated_by" : "5146d03d8aaaaaaaaaaaaabbae60620a5",
  "enabled" : true
} ]
}
```

Status Codes

For details, see [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.6.3 Deleting a User

Function

This API is used to delete an IAM Identity Center user based on the user ID.

URI

DELETE /v1/identity-stores/{identity_store_id}/users/{user_id}

Table 4-267 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the 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 4-268 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 4-269 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403

Table 4-270 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 404**Table 4-271** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.6.4 Querying User Details

Function

This API is used to query details about an IAM Identity Center user based on the user ID.

URI

GET /v1/identity-stores/{identity_store_id}/users/{user_id}

Table 4-272 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the 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 4-273 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 4-274 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 the 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	Name of a user
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	Object that contains the user's work-related information

Table 4-275 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 4-276 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: <ul style="list-style-type: none">• NOT_VERIFIED• VERIFIED

Table 4-277 external_ids

Parameter	Type	Description
id	String	ID issued by an external identity provider Minimum length: 1 Maximum length: 256
issuer	String	Issuer of the external ID Minimum length: 1 Maximum length: 100

Table 4-278 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 name Minimum length: 1 Maximum length: 1024
honorific_suffix	String	Suffix of a user name Minimum length: 1 Maximum length: 1024
middle_name	String	Middle name of a user Minimum length: 1 Maximum length: 1024

Table 4-279 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 4-280 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 4-281 manager

Parameter	Type	Description
value	String	Manager Minimum length: 1 Maximum length: 1024

Status code: 400

Table 4-282 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403**Table 4-283** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 404**Table 4-284** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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-a0aaaa33f",
  "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" : "5146d03d8aaaaaaaaaaaaabbae60620a5",
  "updated_at" : 1687184129926,
  "updated_by" : "5146d03d8aaaaaaaaaaaaabbae60620a5",
  "email_verified" : true,
  "enabled" : true
}
```

Status Codes

For details, see [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.6.5 Updating a User

Function

This API is used to update the attributes of an IAM Identity Center user based on the user ID.

URI

PUT /v1/identity-stores/{identity_store_id}/users/{user_id}

Table 4-285 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the 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 4-286 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 4-287 Parameters in the request body

Parameter	Mandatory	Type	Description
operations	Yes	Array of objects	List of updated user attributes Array length: 1-100

Table 4-288 operations

Parameter	Mandatory	Type	Description
attribute_path	Yes	String	Path of the attribute to be updated Minimum length: 1 Maximum length: 255

Parameter	Mandatory	Type	Description
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 4-289 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403

Table 4-290 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 404

Table 4-291 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.6.6 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.

URI

POST /v1/identity-stores/{identity_store_id}/users/retrieve-user-id

Table 4-292 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source Minimum length: 12 Maximum length: 12

Request Parameters

Table 4-293 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 4-294 Parameters in the request body

Parameter	Mandatory	Type	Description
alternate_identifier	Yes	Object	Alternative identifier

Table 4-295 alternate_identifier

Parameter	Mandatory	Type	Description
external_id	No	Object	ID issued by an external identity provider
unique_attribute	No	Object	Unique attribute of a specific principal

Table 4-296 alternate_identifier.external_id

Parameter	Mandatory	Type	Description
id	Yes	String	ID issued by an external identity provider Minimum length: 1 Maximum length: 256
issuer	Yes	String	Issuer of the external ID Minimum length: 1 Maximum length: 100

Table 4-297 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 4-298 Parameters in the response body

Parameter	Type	Description
identity_store_id	String	Globally unique ID of the 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

Status code: 400

Table 4-299 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403**Table 4-300** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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" : {
    "external_id" : null,
    "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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.7 Group Management

4.7.1 Creating a Group

Function

This API is used to create an IAM Identity Center group in the specified identity source.

URI

POST /v1/identity-stores/{identity_store_id}/groups

Table 4-301 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source Minimum length: 12 Maximum length: 12

Request Parameters

Table 4-302 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 4-303 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 4-304 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 the identity source Minimum length: 1 Maximum length: 36

Status code: 400

Table 4-305 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403

Table 4-306 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 409**Table 4-307** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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-c222aaaaaf31a",
  "identity_store_id": "d-a00aaaa33f"
}
```

Status Codes

For details, see [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.7.2 Listing Groups

Function

This API is used to list the IAM Identity Center groups in the specified identity source.

URI

GET /v1/identity-stores/{identity_store_id}/groups

Table 4-308 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source Minimum length: 12 Maximum length: 12

Table 4-309 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 4-310 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 4-311 Parameters in the response body

Parameter	Type	Description
groups	Array of objects	Listed groups
page_info	Object	Pagination information

Table 4-312 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 IDs issued by an external identity provider Array length: 0-10

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 the 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 4-313 groups.external_ids

Parameter	Type	Description
id	String	ID issued by an external identity provider Minimum length: 1 Maximum length: 256
issuer	String	Issuer of the external ID Minimum length: 1 Maximum length: 100

Table 4-314 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 4-315 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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	Request ID
encoded_authentication_message	String	Authentication information

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-c222aaaaaf31a",
    "identity_store_id": "d-a00aaaa33f",
    "created_at": 1677175760379,
    "created_by": "5146d03d8aaaaaaaaaaaaabbae60620a5",
    "updated_at": 1677175760379,
    "updated_by": "5146d03d8aaaaaaaaaaaaabbae60620a5"
  } ],
  "page_info": {
    "next_marker": null,
    "current_count": 1
  }
}
```

```
}  
}
```

Status Codes

For details, see [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.7.3 Deleting a Group

Function

This API is used to delete an IAM Identity Center group based on the group ID.

URI

DELETE /v1/identity-stores/{identity_store_id}/groups/{group_id}

Table 4-317 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the 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 4-318 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 4-319 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403

Table 4-320 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 404

Table 4-321 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.7.4 Updating a Group

Function

This API is used to update the attributes of an IAM Identity Center group based on the group ID.

URI

```
PUT /v1/identity-stores/{identity_store_id}/groups/{group_id}
```

Table 4-322 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the 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 4-323 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 4-324 Parameters in the request body

Parameter	Mandatory	Type	Description
operations	Yes	Array of objects	List of updated group attributes Array length: 1-100

Table 4-325 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

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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.7.5 Querying Group Details

Function

This API is used to query details about an IAM Identity Center group based on the group ID.

URI

GET /v1/identity-stores/{identity_store_id}/groups/{group_id}

Table 4-326 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the 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 4-327 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 4-328** 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 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 the 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 4-329 external_ids

Parameter	Type	Description
id	String	ID issued by an external identity provider Minimum length: 1 Maximum length: 256
issuer	String	Issuer of the 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": "5146d03d8aaaaaaaaaaaaabbae60620a5",
  "updated_at": 1677175760379,
  "updated_by": "5146d03d8aaaaaaaaaaaaabbae60620a5"
}
```

Status Codes

For details, see [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.7.6 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.

URI

POST /v1/identity-stores/{identity_store_id}/groups/retrieve-group-id

Table 4-330 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source Minimum length: 12 Maximum length: 12

Request Parameters

Table 4-331 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 4-332 Parameters in the request body

Parameter	Mandatory	Type	Description
alternate_identifier	Yes	Object	Alternative identifier

Table 4-333 alternate_identifier

Parameter	Mandatory	Type	Description
external_id	No	Object	ID issued by an external identity provider
unique_attribute	No	Object	Unique attribute of a specific principal

Table 4-334 alternate_identifier.external_id

Parameter	Mandatory	Type	Description
id	Yes	String	ID issued by an external identity provider Minimum length: 1 Maximum length: 256
issuer	Yes	String	Issuer of the external ID Minimum length: 1 Maximum length: 100

Table 4-335 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 4-336 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 the identity source Minimum length: 1 Maximum length: 36

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	Request ID
encoded_authentication_message	String	Authentication information

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	Request ID
encoded_authentication_message	String	Authentication information

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" : {
    "external_id" : null,
    "unique_attribute" : {
      "attribute_path" : "display_name",
      "attribute_value" : "Group name g1"
    }
  }
}
```

Example Response

Status code: 200

Successful

```
{
  "group_id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaaaf31a",
  "identity_store_id" : "d-a00aaaa33f"
}
```


Status Codes

For details, see [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.8 Group Membership Management

4.8.1 Adding a User to a Group

Function

This API is used to add a user to a group in the same identity source.

URI

POST /v1/identity-stores/{identity_store_id}/group-memberships

Table 4-339 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source Minimum length: 12 Maximum length: 12

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. Maximum length: 2048

Table 4-341 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 4-342 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 4-343 Parameters in the response body

Parameter	Type	Description
identity_store_id	String	Globally unique ID of the identity source Minimum length: 1 Maximum length: 36
membership_id	String	Globally unique ID of the group membership in the identity source Minimum length: 1 Maximum length: 47

Status code: 400

Table 4-344 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403

Table 4-345 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.8.2 Listing Users in a Group

Function

This API is used to list users in a group based on the group ID.

URI

GET /v1/identity-stores/{identity_store_id}/group-memberships

Table 4-346 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source Minimum length: 12 Maximum length: 12

Table 4-347 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
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 4-348 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. Maximum length: 2048

Response Parameters

Status code: 200

Table 4-349 Parameters in the response body

Parameter	Type	Description
group_memberships	Array of objects	Listed group members
page_info	Object	Pagination information

Table 4-350 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 the identity source Minimum length: 1 Maximum length: 36
member_id	Object	Group member ID
membership_id	String	Globally unique ID of the association between a user and a group in the identity source Minimum length: 1 Maximum length: 47

Table 4-351 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 4-352 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-c222aaaaaf31a",
    "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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.8.3 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.

URI

GET /v1/identity-stores/{identity_store_id}/group-memberships-for-member

Table 4-353 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source Minimum length: 12 Maximum length: 12

Table 4-354 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 4-355 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 4-356 Parameters in the response body

Parameter	Type	Description
group_memberships	Array of objects	Listed group members
page_info	Object	Pagination information

Table 4-357 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 the identity source
member_id	Object	Group member ID
membership_id	String	Globally unique ID of the group membership in the identity source

Table 4-358 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 4-359 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 4-360** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403**Table 4-361** 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_authentication_message	String	Authentication information

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-c222aaaaaf31a",
    "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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.8.4 Removing a User from a Group

Function

This API is used to remove a user from a group based on the group membership ID.

URI

```
DELETE /v1/identity-stores/{identity_store_id}/group-memberships/
{membership_id}
```

Table 4-362 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source Minimum length: 12 Maximum length: 12
membership_id	Yes	String	Globally unique ID of the group membership in the identity source Minimum length: 1 Maximum length: 64

Request Parameters

Table 4-363 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 4-364 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403

Table 4-365 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.8.5 Querying the Group Membership

Function

This API is used to query details about the group membership based on the group membership ID.

URI

```
GET /v1/identity-stores/{identity_store_id}/group-memberships/{membership_id}
```

Table 4-366 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source Minimum length: 12 Maximum length: 12

Parameter	Mandatory	Type	Description
membership_id	Yes	String	Globally unique ID of the group membership in the identity source Minimum length: 1 Maximum length: 64

Request Parameters

Table 4-367 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 4-368 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 the identity source Minimum length: 1 Maximum length: 36
member_id	Object	Group member ID
membership_id	String	Globally unique ID of the group membership in the identity source Minimum length: 1 Maximum length: 47

Table 4-369 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 4-370** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403**Table 4-371** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.8.6 Querying the Group Membership ID

Function

This API is used to query the group membership ID based on the user ID and group ID.

URI

POST /v1/identity-stores/{identity_store_id}/group-memberships/retrieve-group-membership-id

Table 4-372 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source Minimum length: 12 Maximum length: 12

Request Parameters

Table 4-373 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 4-374 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 4-375 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 4-376 Parameters in the response body

Parameter	Type	Description
identity_store_id	String	Globally unique ID of the identity source

Parameter	Type	Description
membership_id	String	Globally unique ID of the group membership in the identity source

Status code: 400**Table 4-377** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403**Table 4-378** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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-c222aaaaaf31a",
  "member_id" : {
    "user_id" : "ac6aa714-daa7-1aaa-aaa2-6715aaaa4dd9"
  }
}
```

Example Response

Status code: 200

Successful

```
{
  "identity_store_id" : "d-a0aaaa33f",
  "membership_id" : "2b0aa970-7aa4-3aaf-0aae-7a2eaaaae3a5"
}
```

Status Codes

For details, see [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.8.7 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.

URI

POST /v1/identity-stores/{identity_store_id}/is-member-in-groups

Table 4-379 Path parameters

Parameter	Mandatory	Type	Description
identity_store_id	Yes	String	Globally unique ID of the identity source Minimum length: 12 Maximum length: 12

Request Parameters

Table 4-380 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 4-381 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 4-382 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 4-383 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 4-384 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

Parameter	Type	Description
membership_exists	Boolean	Whether a user is in a group

Table 4-385 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 4-386** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 403**Table 4-387** Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

Status code: 404

Table 4-388 Parameters in the response body

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message
request_id	String	Request ID
encoded_authentication_message	String	Authentication information

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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.9 SCIM User Management

4.9.1 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 4-389 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant

Request Parameters

Table 4-390 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Table 4-391 Parameters in the request body

Parameter	Mandatory	Type	Description
externalId	No	String	External ID
userName	No	String	Username, which uniquely identifies a user
name	No	Object	Name of a user
displayName	No	String	Display name of a user
nickName	No	String	Nickname of a user
profileUrl	No	String	URL associated with a user
emails	No	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

Parameter	Mandatory	Type	Description
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	No	Array of strings	Summary
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User	No	Object	Object that contains the user's work-related information

Table 4-392 name

Parameter	Mandatory	Type	Description
formatted	No	String	Formatted name to be displayed
familyName	No	String	Family name of a user
givenName	No	String	Given name of a user
middleName	No	String	Middle name of a user
honorificPrefix	No	String	Prefix of a user name
honorificSuffix	No	String	Suffix of a user name

Table 4-393 emails

Parameter	Mandatory	Type	Description
value	Yes	String	Email address
type	No	String	Email address type

Parameter	Mandatory	Type	Description
primary	Yes	Boolean	Whether the value is the user's primary email address

Table 4-394 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 4-395 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 4-396 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

Parameter	Mandatory	Type	Description
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 4-397 manager

Parameter	Mandatory	Type	Description
value	No	String	Manager Minimum length: 1 Maximum length: 1024

Response Parameters

Status code: 201

Table 4-398 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

Parameter	Type	Description
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	Object that contains the user's work-related information

Table 4-399 meta

Parameter	Type	Description
resourceType	String	Resource type
created	String	Resource creation time
lastModified	String	Last resource update time

Table 4-400 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

Parameter	Type	Description
honorificSuffix	String	Suffix of a user name

Table 4-401 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 4-402 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 4-403 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 4-404 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 4-405 manager

Parameter	Type	Description
value	String	Manager Minimum length: 1 Maximum length: 1024

Status code: 400**Table 4-406** 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 4-407** 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 4-408** 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 4-409** 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 4-410** 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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.9.2 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 4-411 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant

Request Parameters

Table 4-412 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Response Parameters

Status code: 200

Table 4-413 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

Parameter	Type	Description
Resources	Array of objects	User information

Table 4-414 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	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

Parameter	Type	Description
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 4-415 Resources.meta

Parameter	Type	Description
resourceType	String	Resource type
created	String	Resource creation time
lastModified	String	Last resource update time

Table 4-416 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 name
honorificSuffix	String	Suffix of a user name

Table 4-417 Resources.emails

Parameter	Type	Description
value	String	Email address
type	String	Email address type

Parameter	Type	Description
primary	Boolean	Whether the value is the user's primary email address

Table 4-418 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	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 4-419 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 4-420 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 4-421 manager

Parameter	Type	Description
value	String	Manager Minimum length: 1 Maximum length: 1024

Status code: 400**Table 4-422** 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 4-423** 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 4-424** 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 4-425** 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 4-426** 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" : "649040aaaaaaaaaaaa3e3050",
  "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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.9.3 Querying User Details

Function

This API is used to query user details.

URI

GET `/{tenant_id}/scim/v2/Users/{user_id}`

Table 4-427 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 4-428 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Response Parameters

Status code: 200

Table 4-429 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
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

Parameter	Type	Description
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 4-430 meta

Parameter	Type	Description
resourceType	String	Resource type
created	String	Resource creation time
lastModified	String	Last resource update time

Table 4-431 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 name
honorificSuffix	String	Suffix of a user name

Table 4-432 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 4-433 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	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

Parameter	Type	Description
type	String	Address type Minimum length: 1 Maximum length: 1024
primary	Boolean	Whether the address is the user's primary address

Table 4-434 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 4-435 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

Parameter	Type	Description
organization	String	Organization Minimum length: 1 Maximum length: 1024

Table 4-436 manager

Parameter	Type	Description
value	String	Manager Minimum length: 1 Maximum length: 1024

Status code: 400**Table 4-437** 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 4-438** 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 4-439** 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 4-440** 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 4-441** 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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.9.4 Deleting a User

Function

This API is used to delete a user.

URI

```
DELETE /{tenant_id}/scim/v2/Users/{user_id}
```

Table 4-442 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 4-443 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Response Parameters

Status code: 400

Table 4-444 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 4-445 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: 404**Table 4-446** 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 4-447** 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 4-448** 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

Example Request

Deleting a user

```
DELETE https://{hostname}/{tenant_id}/scim/v2/Users/{user_id}
```

Example Response

None

Status Codes

For details, see [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.9.5 Updating a User

Function

This API is used to update a user.

URI

```
PUT /{tenant_id}/scim/v2/Users/{user_id}
```

Table 4-449 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 4-450 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Table 4-451 Parameters in the request body

Parameter	Mandatory	Type	Description
id	No	String	Globally unique ID of a user
externalId	No	String	External ID
userName	No	String	Username, which uniquely identifies a user
name	No	Object	Name of a user
displayName	No	String	Display name of a user
nickName	No	String	Nickname of a user
profileUrl	No	String	URL associated with a user
emails	No	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	No	Array of strings	Summary
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User	No	Object	Object that contains the user's work-related information

Table 4-452 name

Parameter	Mandatory	Type	Description
formatted	No	String	Formatted name to be displayed

Parameter	Mandatory	Type	Description
familyName	No	String	Family name of a user
givenName	No	String	Given name of a user
middleName	No	String	Middle name of a user
honorificPrefix	No	String	Prefix of a user name
honorificSuffix	No	String	Suffix of a user name

Table 4-453 emails

Parameter	Mandatory	Type	Description
value	Yes	String	Email address
type	No	String	Email address type
primary	Yes	Boolean	Whether the value is the user's primary email address

Table 4-454 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 4-455 phoneNumbers

Parameter	Mandatory	Type	Description
value	No	String	Phone number

Parameter	Mandatory	Type	Description
type	No	String	Phone number type
primary	No	Boolean	Whether the value is the user's primary phone number

Table 4-456 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 4-457 manager

Parameter	Mandatory	Type	Description
value	No	String	Manager Minimum length: 1 Maximum length: 1024

Response Parameters

Status code: 200

Table 4-458 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
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	Object that contains the user's work-related information

Table 4-459 meta

Parameter	Type	Description
resourceType	String	Resource type
created	String	Resource creation time

Parameter	Type	Description
lastModified	String	Last resource update time

Table 4-460 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 4-461 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 4-462 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

Parameter	Type	Description
primary	Boolean	Whether the address is the user's primary address

Table 4-463 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 4-464 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 4-465 manager

Parameter	Type	Description
value	String	Manager Minimum length: 1 Maximum length: 1024

Status code: 400**Table 4-466** 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 4-467** 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 4-468** 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 4-469** 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 4-470** 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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.9.6 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 4-471 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 4-472 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Table 4-473 Parameters in the request body

Parameter	Mandatory	Type	Description
schemas	No	Array of strings	Summary
Operations	No	Array of objects	List of the updates to be performed

Table 4-474 Operations

Parameter	Mandatory	Type	Description
op	No	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	String	Attribute value. You do not need to set this parameter if you intend to remove an attribute.

Response Parameters

Status code: 200

Table 4-475 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
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 4-476 meta

Parameter	Type	Description
resourceType	String	Resource type
created	String	Resource creation time

Parameter	Type	Description
lastModified	String	Last resource update time

Table 4-477 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 4-478 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 4-479 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

Parameter	Type	Description
primary	Boolean	Whether the address is the user's primary address

Table 4-480 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 4-481 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 4-482 manager

Parameter	Type	Description
value	String	Manager Minimum length: 1 Maximum length: 1024

Status code: 400**Table 4-483** 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 4-484** 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 4-485** 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 4-486** 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 4-487** 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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.10 SCIM Group Management

4.10.1 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 4-488 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant

Request Parameters

Table 4-489 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Table 4-490 Parameters in the request body

Parameter	Mandatory	Type	Description
externalId	No	String	External ID
displayName	No	String	Display name of a group
members	No	Array of objects	List of member objects in a group
schemas	No	Array of strings	Summary

Table 4-491 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 4-492 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
displayName	String	Display name of a group
members	Array of objects	Members in a group

Table 4-493 meta

Parameter	Type	Description
resourceType	String	Resource type
created	String	Resource creation time
lastModified	String	Last resource update time

Table 4-494 members

Parameter	Type	Description
value	String	Globally unique ID of a member
\$ref	String	Reference information of a member

Parameter	Type	Description
type	String	Member type. User: user

Status code: 400**Table 4-495** 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 4-496** 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 4-497** 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: 409**Table 4-498** 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 4-499** 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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.10.2 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 4-500 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant

Request Parameters

Table 4-501 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Response Parameters

Status code: 200

Table 4-502 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 4-503 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 4-504 Resources.meta

Parameter	Type	Description
resourceType	String	Resource type
created	String	Resource creation time
lastModified	String	Last resource update time

Table 4-505 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 4-506** 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 4-507** 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: 404**Table 4-508** 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 4-509** 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 4-510** 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

Example Request

Listing groups

```
GET https://{hostname}/{tenant_id}/scim/v2/Groups
```

Example Response

Status code: 200

Successful

```
{
  "totalResults" : 1,
  "itemsPerPage" : 10,
  "startIndex" : "649040aaaaaaaaaaaa3e3050",
  "schemas" : [ "urn:ietf:params:scim:api:messages:2.0:ListResponse" ],
  "Resources" : [ {
    "id" : "0efaa0db-6aa4-7aaa-6aa5-c222aaaf31a",
    "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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.10.3 Querying Group Details

Function

This API is used to query group details.

URI

```
GET /{tenant_id}/scim/v2/Groups/{group_id}
```

Table 4-511 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 4-512 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Response Parameters

Status code: 200

Table 4-513 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
displayName	String	Display name of a group
members	Array of objects	Members in a group

Table 4-514 meta

Parameter	Type	Description
resourceType	String	Resource type
created	String	Resource creation time
lastModified	String	Last resource update time

Table 4-515 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 4-516** 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 4-517** 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 4-518** 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 4-519** 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 4-520** 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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.10.4 Deleting a Group

Function

This API is used to delete a group.

URI

DELETE /{tenant_id}/scim/v2/Groups/{group_id}

Table 4-521 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 4-522 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Response Parameters

Status code: 400

Table 4-523 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 4-524 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 4-525 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: 409**Table 4-526** 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 4-527** 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 group

```
DELETE https://{hostname}/{tenant_id}/scim/v2/Groups/{group_id}
```

Example Response

None

Status Codes

For details, see [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.10.5 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 4-528 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 4-529 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Table 4-530 Parameters in the request body

Parameter	Mandatory	Type	Description
schemas	No	Array of strings	Summary
Operations	No	Array of objects	List of the updates to be performed

Table 4-531 Operations

Parameter	Mandatory	Type	Description
op	Yes	String	Update type. add : add an attribute; replace : replace an attribute; remove : remove an attribute.
value	Yes	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 and members.

Response Parameters

Status code: 400

Table 4-532 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 4-533 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 4-534** 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 4-535** 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 4-536** 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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.11 Service Provider (SP) Management

4.11.1 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 4-537 Path parameters

Parameter	Mandatory	Type	Description
tenant_id	Yes	String	Globally unique ID of a tenant

Request Parameters

Table 4-538 Parameters in the request header

Parameter	Mandatory	Type	Description
Authorization	Yes	String	Bearer token

Response Parameters

Status code: 200

Table 4-539 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 4-540 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 4-541 patch

Parameter	Type	Description
supported	Boolean	Whether an SP supports the operation

Table 4-542 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 4-543 filter

Parameter	Type	Description
supported	Boolean	Whether an SP supports the operation
maxResults	Integer	Maximum number of results

Table 4-544 changePassword

Parameter	Type	Description
supported	Boolean	Whether an SP supports the operation

Table 4-545 sort

Parameter	Type	Description
supported	Boolean	Whether an SP supports the operation

Table 4-546 etag

Parameter	Type	Description
supported	Boolean	Whether an SP supports the operation

Status code: 400**Table 4-547** 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 4-548** 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: 404**Table 4-549** 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 4-550** 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 4-551** 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

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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.12 Client Management

4.12.1 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 4-552 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: <ul style="list-style-type: none">• public
token_endpoint_auth_method	Yes	String	Authentication method required to send a request to the token endpoint Enumerated value: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• urn:ietf:params:oauth:grant-type:device_code• authorization_code

Parameter	Mandatory	Type	Description
response_types	Yes	Array of strings	OAuth2.0 authorization type that a client can use at the authorization endpoint Enumerated value: <ul style="list-style-type: none">code

Response Parameters

Status code: 200

Table 4-553 Parameters in the response body

Parameter	Type	Description
client_info	Object	Client registration information

Table 4-554 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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.13 Token Management

4.13.1 Creating a Token

Function

This API is used to create an access token.

URI

POST /v1/tokens

Request Parameters

Table 4-555 Parameters in the request body

Parameter	Mandatory	Type	Description
client_id	Yes	String	Unique ID of the client

Parameter	Mandatory	Type	Description
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.
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: <ul style="list-style-type: none">• 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 4-556 Parameters in the response body

Parameter	Type	Description
token_info	Object	Token information

Table 4-557 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
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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.14 Device Authorization Management

4.14.1 Requesting Device Authorization

Function

This API is used to request device authorization.

URI

POST /v1/device/authorize

Request Parameters

Table 4-558 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 4-559 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)

Parameter	Type	Description
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
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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.15 Authorization Management

4.15.1 Logging Out of a User

Function

This API is used to log a user out of the portal.

URI

GET /v1/logout

Request Parameters

None

Response Parameters

None

Example Request

This API is used to log out of a user.

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

Example Response

None

Status Codes

For details, see [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.16 Account Management

4.16.1 Listing Accounts

Function

This API is used to list all accounts assigned to a user.

URI

GET /v1/assigned-accounts

Table 4-560 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 4-561 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 4-562 Parameters in the response body

Parameter	Type	Description
account_list	Array of objects	Listed accounts
page_info	Object	Pagination information

Table 4-563 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 4-564 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" : "5146d03d8aaaaaaaaaaaaabbae60620a5",
    "account_name" : "example-account-name",
    "email_address" : "email@example.com"
  } ],
  "page_info" : {
    "next_marker" : null,
    "current_count" : 1
  }
}
```

Status Codes

For details, see [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.17 Agency Management

4.17.1 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 4-565 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 4-566 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 4-567 Parameters in the response body

Parameter	Type	Description
agency_list	Array of objects	Listed agencies or trust agencies
page_info	Object	Pagination information

Table 4-568 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 4-569 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": "5146d03d8aaaaaaaaaaaaabbae60620a5",
    "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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

4.18 Credentials Management

4.18.1 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 4-570 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 4-571 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 4-572** Parameters in the response body

Parameter	Type	Description
agency_credentials	Object	Credential of an agency or trust agency assigned to a user

Table 4-573 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 [Status Codes](#).

Error Codes

For details, see [Error Codes](#).

5 Appendixes

5.1 Status Codes

Table 5-1 Status codes

Status Code	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 Code	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 Code	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 Code	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	IdentityCenter.400	Bad Request: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
404	IdentityCenter.400	Bad Request: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
404	IdentityCenter.404	Not Found: {0}.	Resource not found.	Check whether the resource exists.
403	IdentityCenter.1000	No permission for action {0}.	Insufficient permissions.	Check whether you have required permissions.
403	IdentityCenter.1001	Access denied: {0}	The dependent API cannot be accessed.	Check whether you have required and dependent permissions.
404	IdentityCenter.1002	Bad Request: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
403	IdentityCenter.1003	Bad Request: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
403	IdentityCenter.1004	Bad Request: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
409	IdentityCenter.1006	Concurrency conflicts. Try again later.	Concurrency conflicts. Try again later.	Check whether the request parameters conflict and try again.
409	IdentityCenter.1007	Data modification failed.	Modification failed.	Check whether any data conflicts occur.

Status Code	Error Code	Error Message	Description	Solution
409	IdentityCenter.1204	The permission set already exists.	Permission set already created.	Check whether the permission set has already been created.
404	IdentityCenter.1205	The permission set does not exist.	Permission set not found.	Check whether the permission set exists.
409	IdentityCenter.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	IdentityCenter.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	IdentityCenter.1209	Bad Request:{0}.	Organizations operation error.	Contact technical support.
400	IdentityCenter.1210	Account not found.	Account not found.	Check whether the account exists and is managed in Organizations.
409	IdentityCenter.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	IdentityCenter.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	IdentityCenter.1212	Request ID not found.	Request identified by the ID not found.	Check whether the request ID is correct.

Status Code	Error Code	Error Message	Description	Solution
400	IdentityCenter.1214	Region not registered in the service.	Region not registered.	Check whether the region has been registered.
403	IdentityCenter.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.
409	IdentityCenter.1216	Only one region can be registered.	Only one region can be registered.	Check whether another region has been registered.
404	IdentityCenter.1217	HTTP request header {0} not found.	HTTP request header not found.	Check whether the required HTTP request header is contained.
400	IdentityCenter.1218	Invalid X-Request-Proof request header.	Invalid request proof header.	Check whether the request proof header is correct.
400	IdentityCenter.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	IdentityCenter.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	IdentityCenter.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.

Status Code	Error Code	Error Message	Description	Solution
400	IdentityCenter.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	IdentityCenter.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	IdentityCenter.1223	Organizations not enabled.	Organizations not enabled.	Enable Organizations first.
404	IdentityCenter.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	IdentityCenter.1227	Identity store creation failed.	Failed to create the identity source.	Check whether the request parameter is correct.
500	IdentityCenter.1227	Identity store creation failed.	Failed to create the identity source.	Contact technical support.
400	IdentityCenter.1228	Identity store deletion failed.	Failed to delete the identity source.	Check whether the request parameter is correct.
500	IdentityCenter.1229	No service instance can be deleted.	Failed to delete the identity source.	Contact technical support.
400	IdentityCenter.1230	Service-linked agency deletion failed.	Failed to delete the service-linked agency.	Check whether the request parameter is correct.

Status Code	Error Code	Error Message	Description	Solution
400	IdentityCenter.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	IdentityCenter.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	IdentityCenter.1236	Invalid {0}	Invalid parameter.	Check whether the request parameter is valid.
403	IdentityCenter.1242	please open the service instance first!	Service instance not enabled.	Enable the service instance first.
400	IdentityCenter.1243	Failed to create the trust agency.	Failed to create the trust agency.	Check whether the request parameter is correct.
400	IdentityCenter.1244	Authentication failed.	Failed to check permissions.	Check whether the request parameter is correct.
403	IdentityCenter.1244	Authentication failed.	Failed to check permissions.	Check whether you have permission to perform this operation.
500	IdentityCenter.1244	Authentication failed.	Failed to check permissions.	Contact technical support.
400	IdentityCenter.1245	Only one instance can be provisioned.	Only one instance can be enabled.	Check whether the instance has been enabled.
400	IdentityCenter.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.

Status Code	Error Code	Error Message	Description	Solution
500	IdentityCenter.1247	Failed to delete the trust agency.	Failed to delete the trust agency.	Contact technical support.
500	IdentityCenter.1248	Failed to query the trust agency.	Failed to query the trust agency.	Contact technical support.
400	IdentityCenter.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	IdentityCenter.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	IdentityCenter.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	IdentityCenter.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	IdentityCenter.1254	No region registered.	Registered region not found.	Check whether the region has been registered.
409	IdentityCenter.1257	Duplicate entity objects.	Duplicate entity objects.	Check whether the data already exists.
400	IdentityCenter.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	IdentityCenter.1259	Service instance not found.	Instance not found.	Check whether the service instance is created.

Status Code	Error Code	Error Message	Description	Solution
500	IdentityCenter.1260	Internal server error.	Internal service error.	Contact technical support.
400	IdentityCenter.1261	Failed to obtain the identity store information.	Failed to query the connected identity source.	Check whether the identity source exists.
404	IdentityCenter.1000	no permission to bind account.	You do not have permission to attach the account.	Check whether the account has been added to Organizations.
409	IdentityCenter.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	IdentityCenter.1261	Permanent delete sdr meter db data field.	Failed to permanently delete data fields from the SDR meter database.	Check whether the SDR meter data exists.
400	IdentityCenter.1263	The account has not applied for OBT.	The account has not applied for OBT.	Apply for an OBT first.
400	IdentityCenter.1264	Account tag query failed.	An error occurred in account tag query.	Check whether the request parameter is correct.
403	IdentityCenter.1265	HTTP request header not found.	HTTP request header not found.	Check whether the required HTTP request header is contained.
400	IdentityCenter.1266	HTTP request header not found.	Invalid HTTP request header.	Check whether the HTTP request header is valid.
400	IdentityCenter.1269	fail request for assume with service principal.	Failed to obtain the agency credential.	Check whether the request parameter is correct.

Status Code	Error Code	Error Message	Description	Solution
403	IdentityCenter.1269	fail request for assume with service principal.	Failed to obtain the agency credential.	Check whether you have permission to perform this operation.
400	IdentityCenter.1270	Failed to obtain the MFA settings of the identity store.	Failed to obtain the MFA settings of the identity source.	Check whether the request parameter is correct.
409	IdentityCenter.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	IdentityCenter.1271	Failed to update the MFA settings of the identity store.	Failed to update the MFA settings of the identity source.	Check whether the request parameter is correct.
409	IdentityCenter.1271	The alias already exists.	Duplicate identity source ID alias.	Change the alias.
403	IdentityCenter.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	IdentityCenter.1273	The identity store 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	IdentityCenter.1273	The operation is not allowed because the account is frozen.	Account frozen. Operation not allowed.	Check whether the account is frozen.
403	IdentityCenter.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	IdentityCenter.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	IdentityCenter.1276	Service instance not found.	Instance not found.	Check whether the request parameter is correct.
404	IdentityCenter.1276	Service instance not found.	Instance not found.	Check whether the instance exists.
400	IdentityCenter.1277	Agency creation failed.	Failed to create the agency.	Check whether the request parameter is correct.
500	IdentityCenter.1278	Agency deletion failed.	Failed to delete the agency.	Contact technical support.
500	IdentityCenter.1279	Role query failed.	Failed to query the policy.	Contact technical support.
500	IdentityCenter.1280	Agency query failed.	Failed to query the agency.	Contact technical support.
404	IdentityCenter.1281	Role ID {roleid} not found.	Role ID {roleid} not found.	Check whether the role ID exists.
409	IdentityCenter.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.

Status Code	Error Code	Error Message	Description	Solution
400	IdentityCenter.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	IdentityCenter.1284	Failed to process Organizations broadcast messages.	An error occurred when IAM Identity Center consumes Organizations events.	Check whether permissions are sufficient.
500	IdentityCenter.1284	Failed to process Organizations broadcast messages.	An error occurred when IAM Identity Center consumes Organizations events.	Contact technical support.
400	IdentityCenter.1285	Custom role creation failed.	Failed to create the custom policy.	Check whether the custom policy is correct.
400	IdentityCenter.1286	Custom role update failed.	Failed to update the custom policy.	Check whether the custom policy is correct.
500	IdentityCenter.1287	Custom role deletion failed.	Failed to delete the custom policy.	Contact technical support.
500	IdentityCenter.1290	Authorization association not found.	Authorization association not found.	Contact technical support.
403	IdentityCenter.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	IdentityCenter.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.

Status Code	Error Code	Error Message	Description	Solution
500	IdentityCenter.1300	Internal server error.	Internal service error.	Contact technical support.
409	IdentityCenter.1301	Failed to create another identity store because an identity store 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	IdentityCenter.1302	Account not found.	No Organizations information found for the account.	Check whether the request parameter is correct.
400	IdentityCenter.1303	Organizations not enabled.	Organizations not enabled.	Enable Organizations first.
500	IdentityCenter.1304	Bad Request: {0}.	Organizations operation error.	Contact technical support.
403	IdentityCenter.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	IdentityCenter.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	IdentityCenter.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.

Status Code	Error Code	Error Message	Description	Solution
400	IdentityCenter.1308	Identity store not found.	Identity source not found.	Check whether the identity source ID is correct.
404	IdentityCenter.1308	Identity store not found.	Identity source not found.	Check whether the identity source exists.
500	IdentityCenter.1309	Failed to obtain the access token.	Failed to obtain the PKI token.	Contact technical support.
400	IdentityCenter.1310	Duplicate username or email address.	Duplicate username or email address.	Try another username or email address.
400	IdentityCenter.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	IdentityCenter.1312	User not found.	User not found.	Check whether the user exists.
404	IdentityCenter.1313	User extended attributes not found.	User extended attributes not found.	Check whether the user attributes are complete.
400	IdentityCenter.1314	Invalid password.	The password complexity does not meet requirements.	Use a more complex password.
400	IdentityCenter.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.

Status Code	Error Code	Error Message	Description	Solution
404	IdentityCenter.1316	Unique user ID not found.	Unique user ID not found.	Check whether the request parameter is correct.
400	IdentityCenter.1317	User disabled.	Repeat disablement.	Check whether the object has already been disabled.
400	IdentityCenter.1318	User enabled.	Repeat enablement.	Check whether the object has already been enabled.
400	IdentityCenter.1319	Login credentials cannot be verified. Please try again.	Incorrect username or password.	Check whether the login credential is correct and try again.
404	IdentityCenter.1319	we couldn't verify your sign-in credentials. please try again.	Username or password not found.	Check whether the username or password exists.
400	IdentityCenter.1320	User disabled.	User disabled.	Check whether the user is enabled.
400	IdentityCenter.1321	duplicate email.	Duplicate email address.	Try another email address.
500	IdentityCenter.1322	Algorithm not found: {0}.	Algorithm not found.	Contact technical support.
400	IdentityCenter.1324	The new password must be different from the username.	The new password must be different from the username.	Enter another password.
400	IdentityCenter.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	IdentyCenter.1326	Internal server error: {0}.	Internal service error.	Contact technical support.
400	IdentyCenter.1327	Invalid metadata.	Invalid SAML metadata.	Check whether the request parameter is correct.
400	IdentyCenter.1328	IdP configuration already exists.	IdP configuration already exists and cannot be created again.	Check whether the IdP configuration already exists.
400	IdentyCenter.1329	The IdP configuration status is incorrect.	The IdP configuration status is incorrect.	Check whether the IdP configuration status is correct.
404	IdentyCenter.1330	IdP configuration not found.	IdP configuration not found.	Check whether the IdP configuration exists.
400	IdentyCenter.1331	IdP tenant already exists.	IdP tenant already exists.	Check whether the IdP tenant already exists.
404	IdentyCenter.1332	Tenant ID not found.	IdP tenant not found.	Check whether the IdP tenant exists.
400	IdentyCenter.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	IdentyCenter.1334	Bearer token ID not found.	Token not found.	Check whether the token exists.
400	IdentyCenter.1335	The maximum number of allowed bearer tokens has been reached.	The maximum number of tokens has been reached.	Check the token quota.

Status Code	Error Code	Error Message	Description	Solution
400	IdentityCenter.1336	Username verification failed.	Incorrect username.	Check whether the request parameter is correct.
403	IdentityCenter.1337	No permission for action {0}.	No sufficient permissions.	Check whether you have permission to perform this operation.
403	IdentityCenter.1338	Request parameter is required.	The parameter value cannot be empty.	Check whether the parameter is correct.
403	IdentityCenter.1339	Service instance not found.	Parameter error. Service instance not found.	Check whether the parameter is correct.
409	IdentityCenter.1341	Duplicate display name of the group.	The display name of the group already exists.	Try another display name.
409	IdentityCenter.1342	Duplicate entity objects.	Failed to insert data into the database.	Check whether the data already exists.
404	IdentityCenter.1343	Group not found.	Group not found.	Check whether the group exists.
400	IdentityCenter.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	IdentityCenter.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.

Status Code	Error Code	Error Message	Description	Solution
404	IdentityCenter.1349	The attribute_path must be unique.	The path attribute must be unique.	Ensure that the path attribute is unique.
400	IdentityCenter.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	IdentityCenter.1352	The identity store 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.
400	IdentityCenter.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	IdentityCenter.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	IdentityCenter.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	IdentityCenter.1372	Group not found.	Group not found.	Check whether the group exists.
404	IdentityCenter.1372	Group not found.	Group not found.	Check whether the group exists.
400	IdentityCenter.1373	User not found.	User not found.	Check whether the user exists.

Status Code	Error Code	Error Message	Description	Solution
404	IdentityCenter.1373	User not found.	User not found.	Check whether the user exists.
404	IdentityCenter.1374	The association between users and group does not exist.	Group membership not found.	Check whether the user is added to the group.
404	IdentityCenter.1375	Group member not found.	Member not found.	Check whether all requested members exist.
400	IdentityCenter.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	IdentityCenter.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	IdentityCenter.1382	Permanent delete db data field.	Failed to permanently delete database data fields.	Check whether the data already exists.
400	IdentityCenter.1383	The account has not applied for OBT.	Beta account ID required.	Use a beta account.
400	IdentityCenter.1384	Account tag query failed.	An error occurred in account tag query.	Check whether the request parameter is correct.
404	IdentityCenter.1385	HTTP request header not found.	HTTP request header not found.	Check whether the required HTTP request header is contained.

Status Code	Error Code	Error Message	Description	Solution
400	IdentityCenter.1386	HTTP request header not found.	Invalid HTTP request header.	Check whether the HTTP request header is valid.
400	IdentityCenter.1387	MFA device {0} not found.	MFA device not found.	Check whether the parameter is correct.
400	IdentityCenter.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	IdentityCenter.1389	Incorrect format of the X-Request-Proof request header.	Incorrect authentication header pattern.	Check whether the authentication header pattern is correct.
404	IdentityCenter.1390	HTTP request header {0} not found.	HTTP request header not found.	Check whether the HTTP request header exists.
400	IdentityCenter.1391	Invalid X-Request-Proof request header.	Incorrect request proof.	Check whether the request header parameter is correct.
400	IdentityCenter.1392	Failed to obtain the identity token.	Failed to obtain the STS credential.	Check whether the request parameter is correct.
403	IdentityCenter.1392	Failed to obtain the identity token.	Failed to obtain the STS credential.	Check whether you have sufficient permissions.
403	IdentityCenter.1393	The operation is not allowed because the account is frozen.	Account frozen. Operation not allowed.	Check whether the account is frozen.

Status Code	Error Code	Error Message	Description	Solution
403	IdentityCenter.1394	The operation is not allowed because the account is restricted.	Account restricted. Operation not allowed.	Check whether the account is restricted.
404	IdentityCenter.1398	Tenant not found.	Tenant not found.	Check whether the tenant exists.
400	IdentityCenter.1399	Failed to obtain the bearer token.	Failed to obtain the bearer token.	Check whether the parameter is correct.
400	IdentityCenter.1400	Bad Request: {0}.	Failed to create an access token.	Check whether the request parameter is correct.
500	IdentityCenter.1402	Bad Request: {0}.	Failed to create an access token.	Contact technical support.
400	IdentityCenter.1404	Access denied: {0}.	Access denied.	Check whether the request parameter is correct.
403	IdentityCenter.1404	Access denied: {0}.	Access denied.	Check whether you have permission to perform this operation.
400	IdentityCenter.1405	Bad Request: {0}.	Failed to verify the request parameter.	Check whether the request parameter is correct.
500	IdentityCenter.1405	Bad Request: {0}.	Failed to verify the request parameter.	Contact technical support.
404	IdentityCenter.1406	not found application.	Application not found.	Check whether the application exists.

Status Code	Error Code	Error Message	Description	Solution
400	IdentityCenter.1407	Failed to request the authorization of the account.	Profile not found.	Check whether the request parameter is correct.
400	IdentityCenter.1409	Invalid token.	Invalid ID token.	Check whether the ID token is valid.
401	IdentityCenter.1410	{0}.	Unauthorized.	Perform authorization as prompted.
401	IdentityCenter.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	IdentityCenter.1411	Client registration error.	An exception occurred when you register the client.	Check whether the request parameter is correct.
500	IdentityCenter.1411	Client registration error.	An exception occurred when you register the client.	Contact technical support.
500	IdentityCenter.1412	Algorithm not found: {0}.	Algorithm not found.	Check whether the algorithm is correct or contact technical support.
400	IdentityCenter.1413	Invalid session state: {0}.	Invalid session state identifier.	Check whether the session status identifier is correct.
400	IdentityCenter.1414	redis error.	Redis operation error.	Check whether the request parameter is correct.
400	IdentityCenter.1415	Failed to obtain the login token: {0}.	Failed to obtain the login token.	Check whether the request parameter is correct.

Status Code	Error Code	Error Message	Description	Solution
500	IdentityCenter.1415	Failed to obtain the login token: {0}.	Failed to obtain the login token.	Contact technical support.
500	IdentityCenter.1416	Internal server error: {0}.	Internal service error.	Contact technical support.
404	IdentityCenter.1417	Identity store ID not found.	Identity source ID not found.	Check whether the identity source ID exists.
400	IdentityCenter.1418	The workflow cannot be created.	Failed to create a workflow.	Check whether the parameter is correct.
400	IdentityCenter.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.
400	IdentityCenter.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	IdentityCenter.1500	Invalid Token.	Invalid access token.	Check whether the access token is valid.
500	IdentityCenter.1501	Failed to obtain the identity token: {0}.	Failed to obtain the identity token.	Contact technical support.
500	IdentityCenter.1502	Failed to list accounts for the user: {0}.	Failed to obtain the account list.	Contact technical support.
500	IdentityCenter.1503	Failed to list agencies for the account: {0}.	Failed to list agencies or trust agencies for the account.	Contact technical support.

Status Code	Error Code	Error Message	Description	Solution
500	IdentityCenter.1504	Token verification failed: {0}.	Failed to verify the access token.	Contact technical support.
400	IdentityCenter.1505	Invalid Param: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
500	IdentityCenter.1506	Algorithm not found.	Algorithm not found.	Check whether the algorithm is correct or contact technical support.
400	IdentityCenter.1507	Failed to obtain the service instance information: {0}.	Failed to obtain the service instance information.	Check whether the request parameter is correct.
500	IdentityCenter.1507	Failed to obtain the service instance information: {0}.	Failed to obtain the service instance information.	Contact technical support.
400	IdentityCenter.1508	Failed to delete the MFA device: {0}.	Failed to delete the MFA device for the user.	Check whether the parameter is correct.
500	IdentityCenter.1508	Failed to delete the MFA device: {0}.	Failed to delete the MFA device for the user.	Contact technical support.
400	IdentityCenter.1509	Failed to create the workflow: {0}.	Failed to create a workflow.	Check whether the parameter is correct.
500	IdentityCenter.1509	Failed to create the workflow: {0}.	Failed to create a workflow.	Contact technical support.
400	IdentityCenter.1511	Failed to obtain the MFA settings: {0}.	Failed to obtain the MFA management settings of the user.	Check whether the parameter is correct.

Status Code	Error Code	Error Message	Description	Solution
500	IdentityCenter.1511	Failed to obtain the MFA settings: {0}.	Failed to obtain the MFA management settings of the user.	Contact technical support.
400	IdentityCenter.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	IdentityCenter.1512	Failed to list MFA devices for the user: {0}.	Failed to list MFA devices for the user.	Contact technical support.
500	IdentityCenter.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	IdentityCenter.1514	Failed to update the MFA device: {0}.	Failed to update MFA devices for the user.	Check whether the parameter is correct.
500	IdentityCenter.1514	Failed to update the MFA device: {0}.	Failed to update MFA devices for the user.	Contact technical support.
400	IdentityCenter.1515	Failed to obtain the permission set.	Failed to obtain the permission set.	Check whether the parameter is correct.
500	IdentityCenter.1515	Failed to obtain the permission set.	Failed to obtain the permission set.	Contact technical support.
400	IdentityCenter.1516	Email verification failed: {0}.	Email verification failed.	Check whether the parameter is correct.

Status Code	Error Code	Error Message	Description	Solution
500	IdentityCenter.1516	Email verification failed: {0}.	Email verification failed.	Contact technical support.
500	IdentityCenter.1517	failed to get the PKI token.	Failed to obtain the PKI token.	Contact technical support.
403	IdentityCenter.1518	read permission does not support MFA registration.	Read permissions do not support MFA binding.	Check whether permissions are sufficient.
403	IdentityCenter.1519	MFA disabled.	MFA disabled.	Enable MFA first.
400	IdentityCenter.1520	Invalid access token.	Invalid access token.	Check whether the access token is valid.
404	IdentityCenter.1600	Client not found.	Client not found.	Check whether the client ID is correct.
403	IdentityCenter.1601	Client expired.	The client has expired.	Check whether the client has expired. If yes, add the client again.
403	IdentityCenter.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	IdentityCenter.1603	Internal server error: {0}.	Internal service error.	Contact technical support.
401	IdentityCenter.1604	Invalid token.	Invalid access token.	Apply for a new access token and try again.

Status Code	Error Code	Error Message	Description	Solution
500	IdentityCenter.1605	Algorithm not found: {0}.	Algorithm not found.	Contact technical support.
400	IdentityCenter.1606	Invalid param: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
403	IdentityCenter.1606	Invalid param: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
404	IdentityCenter.1606	Invalid param: {0}.	Invalid request parameter.	Check whether the request parameter is correct.
400	IdentityCenter.1607	Failed to verify the JWT signature: {0}.	JWT token signature verification error.	Check whether the JWT token is correct.
400	IdentityCenter.1608	Authorization pending exception.	Authorization pending exception.	Try again later.
400	IdentityCenter.1609	The client does not support {0}.	Client not supported.	Check whether the request is correct.
500	IdentityCenter.1610	Internal server error.	Internal service error.	Contact technical support.
500	IdentityCenter.1611	Failed to obtain the access token.	Failed to obtain the access token.	Contact technical support.
401	IdentityCenter.1612	Invalid authorization type.	Invalid authorization type.	Check whether the authorization type is correct.

Status Code	Error Code	Error Message	Description	Solution
404	IdentityCenter.1613	Authorization rejected.	Authorization rejected.	Check whether the user agrees to the authorization.
400	IdentityCenter.1615	Requests of this type are not supported.	Request type not supported.	Check whether the request type is correct.
400	IdentityCenter.1616	The workflow is not supported.	Workflow not supported.	Check whether the workflow steps are correct.
400	IdentityCenter.1617	Failed to parse the ID token.	Failed to parse the ID token.	Check whether the ID token is valid.
400	IdentityCenter.1701	User verification exception.	User verification error.	Check whether the request parameter is correct.
500	IdentityCenter.1701	User verification exception.	User verification error.	Contact technical support.
400	IdentityCenter.1702	Login authentication error.	Login authentication error.	Check whether the authorization code is valid.
400	IdentityCenter.1703	Unsupported encoding.	Unsupported encoding.	Check whether the encoding of the request parameter is correct.
400	IdentityCenter.1704	approve code error.	Authorization code approval error.	Check whether the authorization code is valid.
423	IdentityCenter.1705	User locked.	User locked or disabled.	Unlock or enable the user.

Status Code	Error Code	Error Message	Description	Solution	
	424	IdentityCenter.1706	User expired.	The user password has expired.	Change the user password.
	400	IdentityCenter.1707	Incorrect username, password, or identity store id.	Incorrect username, password, or identity source identifier.	Check whether the username, password, or identity source identifier is correct.
	400	IdentityCenter.1708	An error occurred when obtaining the external IdP.	Failed to obtain the identity provider information.	Check whether the request parameter is correct.
	400	IdentityCenter.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	IdentityCenter.1710	No supported methods.	Unsupported method.	Check whether the request parameter is correct.
	400	IdentityCenter.1711	An error occurred when obtaining SAML metadata.	Failed to obtain the SAML metadata.	Check whether the request parameter is correct.
	400	IdentityCenter.1712	The signature certificate cannot be decoded.	Failed to verify the signature certificate.	Check whether the certificate signature is successful.
	400	IdentityCenter.1714	Incorrect SAML response.	SAML response error.	Check whether the SAML response is correct.
	500	IdentityCenter.1716	Algorithm not found: {0}.	Algorithm not found.	Contact technical support.
	400	IdentityCenter.1717	Session expired.	Session expired.	Check whether the session is valid.

Status Code	Error Code	Error Message	Description	Solution
400	IdentityCenter.1718	Failed to reset the password.	Failed to reset the password.	Check whether the request parameter is valid.
400	IdentityCenter.1719	Username verification failed.	Username verification error.	Check whether the request parameter is correct.
400	IdentityCenter.1721	Session timed out or stopped working. Restart your workflow.	Session timed out or stopped working. Restart your workflow.	Restart your workflow.
400	IdentityCenter.1722	Request cannot be completed. Try again later.	Request cannot be completed. Try again later.	Try again later.
400	IdentityCenter.1724	Failed to process the workflow. Try again later.	Failed to process the workflow. Try again later.	Try again later.
400	IdentityCenter.1725	This operation cannot be performed.	This operation cannot be performed.	Check whether the request parameter is correct.
400	IdentityCenter.1726	Failed to verify the MFA code.	Failed to verify the MFA code.	Check whether the request parameter is valid.
400	IdentityCenter.1727	Failed to create an MFA device: {0}	Failed to create an MFA device.	Check whether the request parameter is correct.
400	IdentityCenter.1728	Failed to update the MFA device: {0}	Failed to update the MFA device.	Check whether the request parameter is correct.
400	IdentityCenter.1728	Failed to find the MFA device: {0}	Failed to find the MFA device.	Ensure that the device exists.

Status Code	Error Code	Error Message	Description	Solution
400	IdentityCenter.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	IdentityCenter.1730	Failed to obtain the service instance information.	Failed to obtain the service instance information.	Check whether the request parameter is correct.
400	IdentityCenter.1731	Invalid session state.	Invalid session state.	Check whether the session has expired.
400	IdentityCenter.1734	User search failed.	Failed to retrieve users.	Check whether the request parameter is correct.
400	IdentityCenter.1735	Incorrect username, password, verification code, or identity store id.	Incorrect username, password, verification code, or identity source ID.	Check whether the username, password, verification code, or identity source ID is correct.
400	IdentityCenter.1736	Workflow creation failed. Try again later.	Workflow creation failed. Try again later.	Try again later.
400	IdentityCenter.1737	Incorrect username, password, verification code, or identity store id.	Incorrect username, password, verification code, or identity source ID.	Check whether the username, password, verification code, or identity source ID is correct.
500	IdentityCenter.1738	Failed to obtain the verification code.	Failed to obtain the verification code.	Contact technical support.
403	IdentityCenter.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.

Status Code	Error Code	Error Message	Description	Solution
400	IdentityCenter.1740	Invalid {0}	Invalid parameter.	Check whether the request parameter is valid.
400	IdentityCenter.1741	Invalid one-time password.	Invalid one-time password.	Check whether the one-time password is valid.
500	IdentityCenter.1750	Algorithm not found: {0}	Algorithm not found.	Contact technical support.
400	IdentityCenter.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.

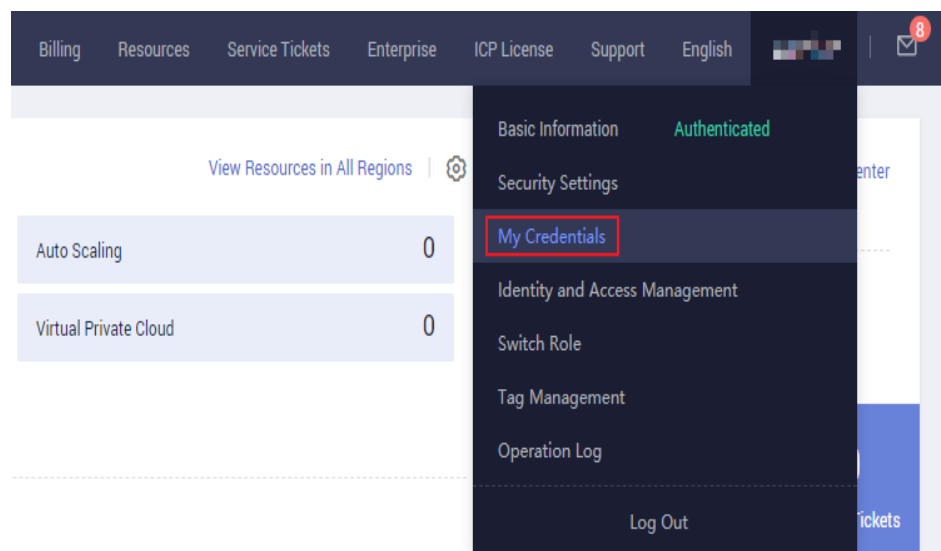
HTTP Status Code	Response Status Code	Error Message	Description	Solution
409	409	Group [{0}] already exists.	Group already exists.	Check whether the group already exists.
500	500	There was an internal server error.	Internal service error.	Contact technical support.

5.3 Obtaining Information About Account, IAM User, Group, Project, Region, and Agency

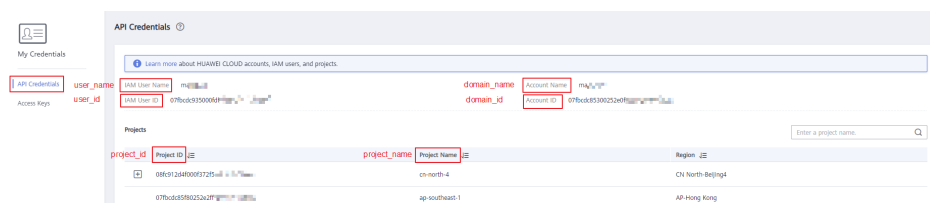
Obtaining Account, IAM User, and Project Information

- 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

6 Change History

Released On	Description
2024-03-29	<p>This issue is the second official release. Modified the following content:</p> <ul style="list-style-type: none">• Added APIs in Access Control Attribute Management.• Added APIs in Querying Details About a Custom Identity Policy.• Added APIs in Adding a Custom Identity Policy.• Added APIs in Deleting a Custom Identity Policy.• Added APIs in Tag Management.
2023-08-30	<p>This issue is the first official release.</p>